Exinda How To Guide:

SQL Access

Exinda ExOS Version 6.4

Copyright

Document Built on August-15-13 at 10:43 AM

Using this guide

Before using this guide, become familiar with the Exinda documentation system.

- "Exinda documentation conventions" on page 2
- "Notes, Tips, Examples, and Cautions" on page 3

Exinda documentation conventions

The Exinda documentation uses the following conventions in the documentation.

Graphical interface conventions

The following is a summary of the conventions used for graphic interfaces such as those in the Exinda Web UI and the Central Management Technical Preview UI.

Convention	Definition
bold	Interface element such as buttons or menus. For example: Select the **Enable** checkbox.
Italics	Reference to other documents. For example: Refer to the *Exinda Application List*.
>	Separates navigation elements. For example: Select **File > Save**.

Command line conventions

The following is a summary of the syntax used for the CLI commands.

```
(config)# command <user input> keyword {list|of|options|to|select|from} [optional
parameter]
```

Convention	Definition
`monospace text`	Command line text or file names
`<courier italics>`	Arguments for which you use values appropriate to your environment.
courier bold	Commands and keywords that you enter exactly as shown.
`[x]`	Enclose an optional keyword or argument.
`{x}`	Enclose a required element, such as a keyword or argument.
`|`	Separates choices within an optional or required element.
`[x {y | z}]`	Braces and vertical lines (pipes) within square brackets indicate a required choice within an optional element.
`command with many parameters that wrap onto two lines in the documentation`	Underlined CLI commands may wrap on the page, but should be entered as a single line.

Notes, Tips, Examples, and Cautions

Throughout the manual the following text styles are used to highlight important points:

- **Notes** include useful features, important issues. They are identified by a light blue background.

  Note Note text

- **Tips** include hints and shortcuts. They are identified by a light blue box.

  Tip Tip text

- **Examples** are presented throughout the manual for deeper understanding of specific concepts. Examples are identified by a light gray background.

  Example

  Text

- **Cautions** and warnings that can cause damage to the device are included when necessary, and are highlighted in yellow.

  Caution Caution text

Table of Contents

Chapter 1: Configure SQL Access

The SQL Access feature on an Exinda appliance provides access to the traffic monitoring database from any ODBC compliant application.

In order to use this feature, SQL access needs to be configured on the Exinda appliance, and an ODBC driver needs to be installed and configured on a client. ODBC aware applications running on the client will then be able to query the Exinda appliance's internal monitoring database.

This How to Guide explains how to configure the Exinda appliance to accept remote SQL connections, as well as setting up the ODBC driver on Windows XP and Windows Vista/7 clients.

Download the ODBC Driver

Download the ODBC driver version that corresponds to your client operating system. Follow the instructions on this site for installing the ODBC driver on your client operating system.

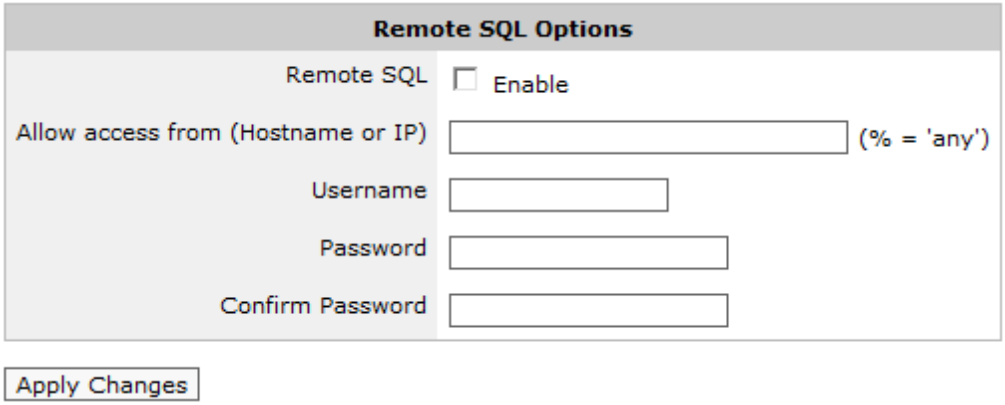
The ODBC driver can be downloaded from:

http://dev.mysql.com/downloads/connector/odbc/

Set Remote SQL Options

In order to allow the Exinda appliance to accept remote SQL connections from an external ODBC connector, you must configure the following settings.

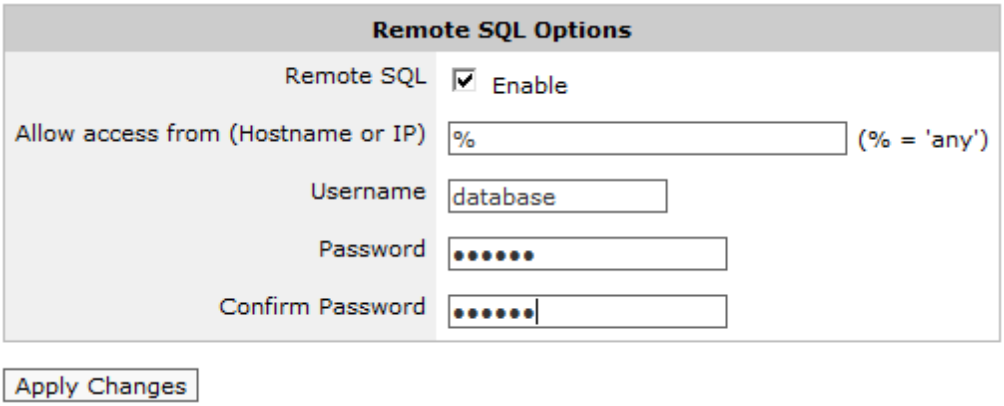
On the Exinda appliance, using the Web User Interface, navigate to System | Setup | SQL Access. You will be presented with the following form.



Remote SQL	Select this option to allow the Exinda appliance to accept remote SQL connections

	from external ODBC connectors.
Allow access from (Hostname or IP)	Use this option to restrict the hosts that can connect to the SQL database. Specify '%' to allow any hosts to connect or enter an IP address or Hostname of a specify host to restrict access.
Username	Specify a username to use for authentication (E.g. 'database').
Password	Specify a password to use for authentication.
Confirm Password	Retype the password specified above.

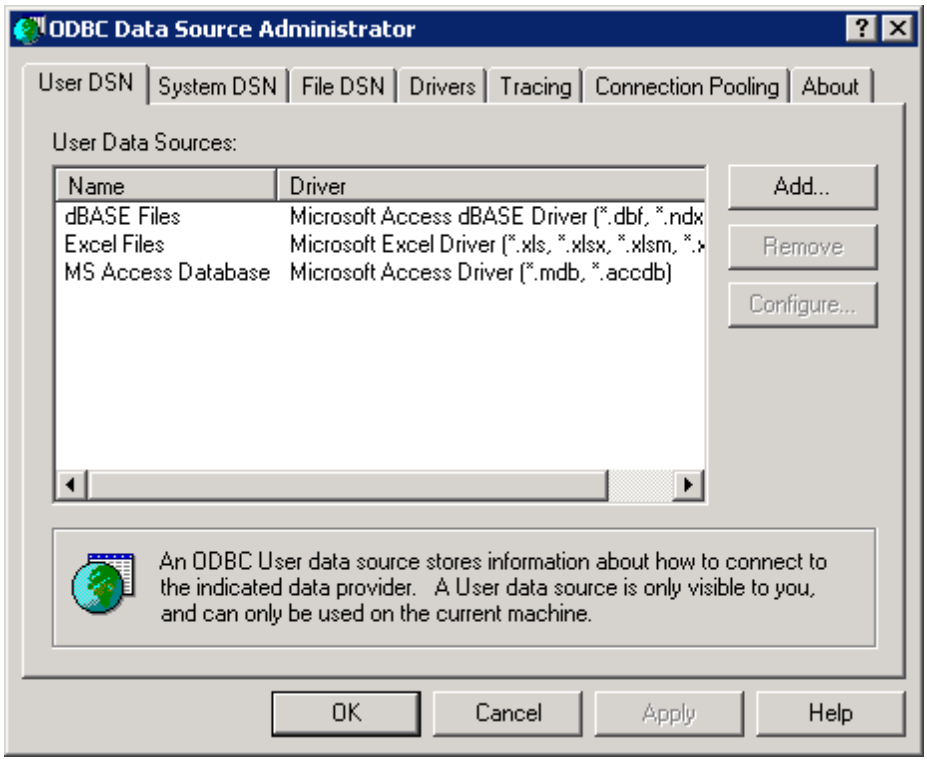
Apply the changes. The SQL access will be made available immediately. A successfully configured appliance would look something like:



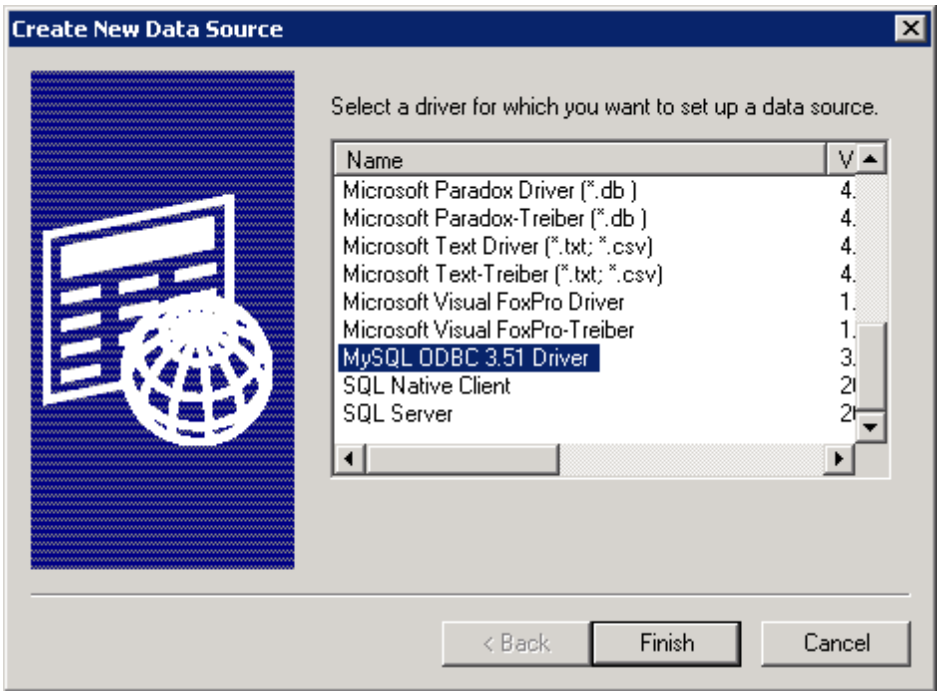
Once remote SQL access has been configured on the Exinda appliance, the next step is to create an ODBC data source on the client.

Create ODBC Data Source on Windows XP

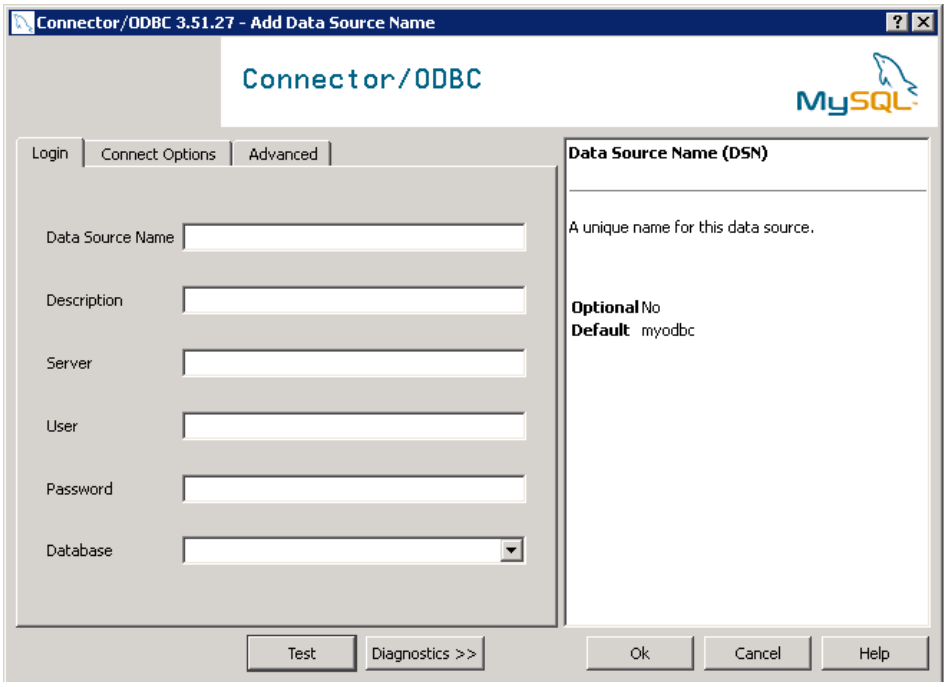
Open **Administrative Tools** and select **Data Sources (ODBC)**. You should be presented with the following dialog.



Select the **User DSN** tab or the **System DSN** tab depending on weather you wish the SQL data to be made available to only the current user (User DSN) or all users (System DSN). Then click **Add...**. This will start a wizard that allows you to create a new data source.

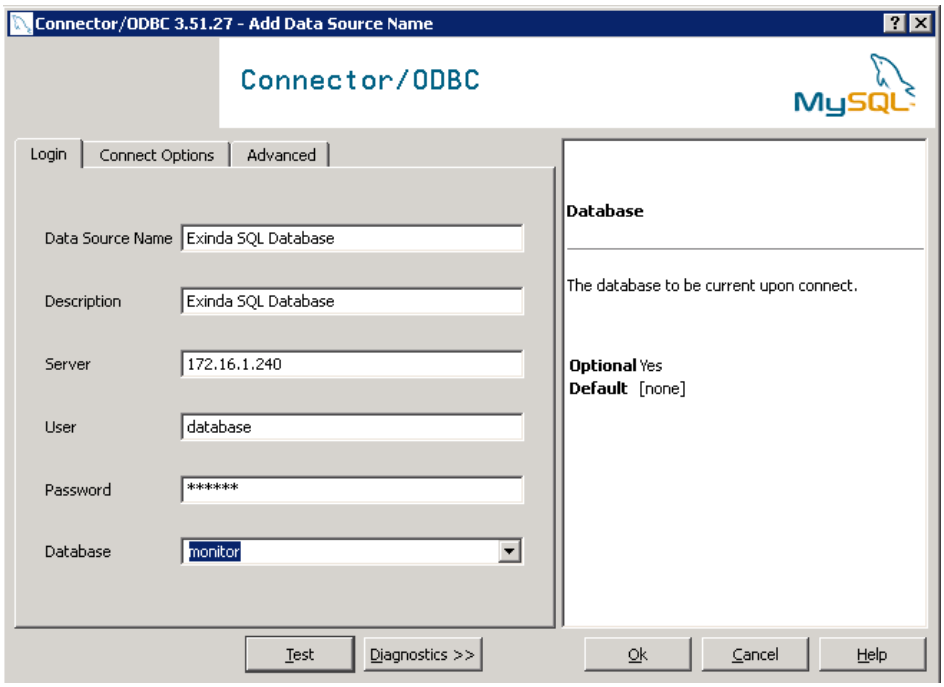


Select **MySQL ODBC Driver** and click **Finish**. You will be prompted to enter details about the SQL access using the form below:

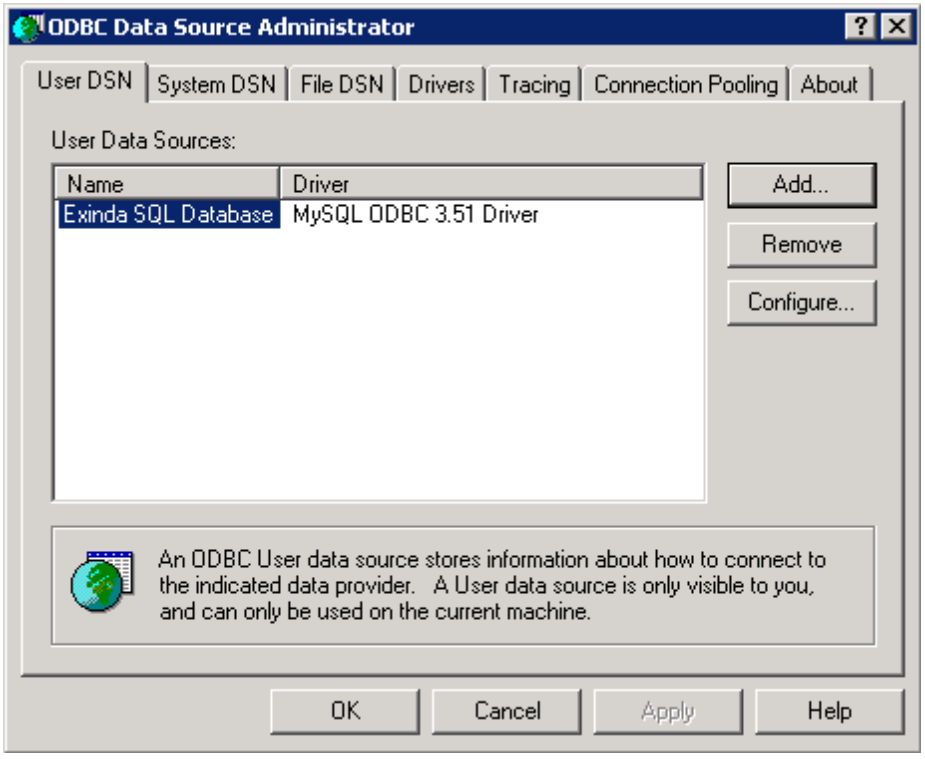


Data Source Name / Description	Enter a descriptive name for the DSN. E.g. 'Exinda SQL Database'.
Server	Enter the IP address of the Exinda appliance.
User	Enter the username you specified when enabling SQL access on the Exinda appliance.
Password	Enter the password you specified when enabling SQL access on the Exinda appliance.
Database	Once the above fields are configured, press the 'Test' button. If the connection attempt is successful, the 'Database' drop down will be populated with a list of available databases. Select 'monitor'.

Here is what a successful configuration looks like:



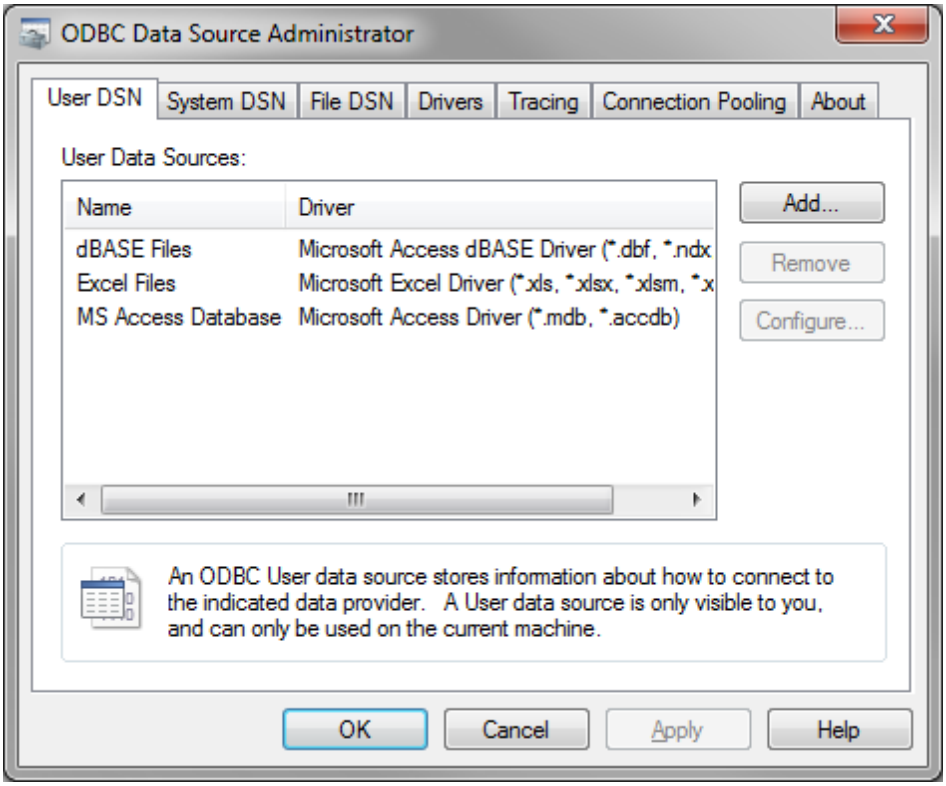
Click **OK**. This will add the 'Exinda SQL Database' to the list of available data sources that can be used by 3rd party applications on this client.



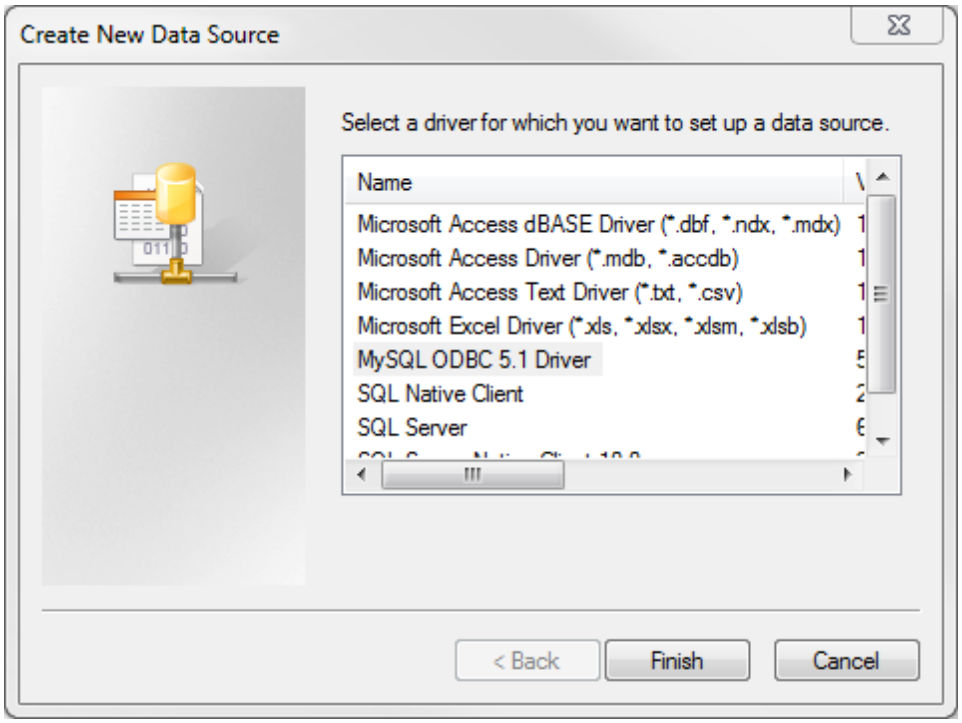
Create ODBC Data Source on Windows 7

Open **Administrative Tools** and select **Data Sources (ODBC)**. You should be presented with the following

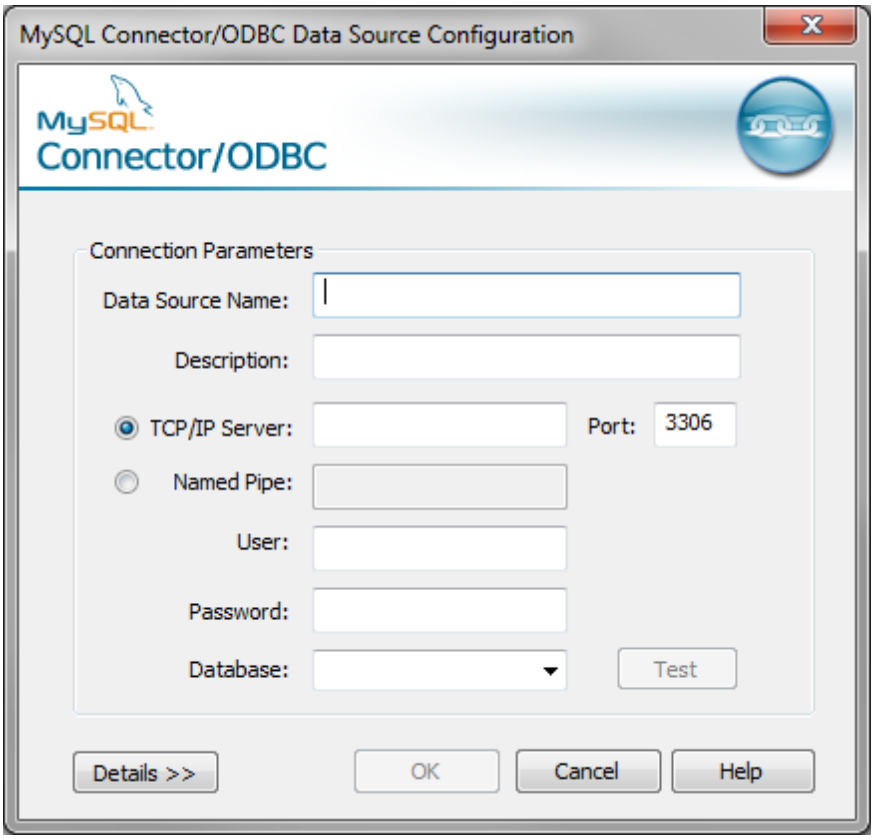
dialog.



Select the **User DSN** tab or the **System DSN** tab depending on weather you wish the SQL data to be made available to only the current user (User DSN) or all users (System DSN). Then click **Add...**. This will start a wizard that allows you to create a new data source.

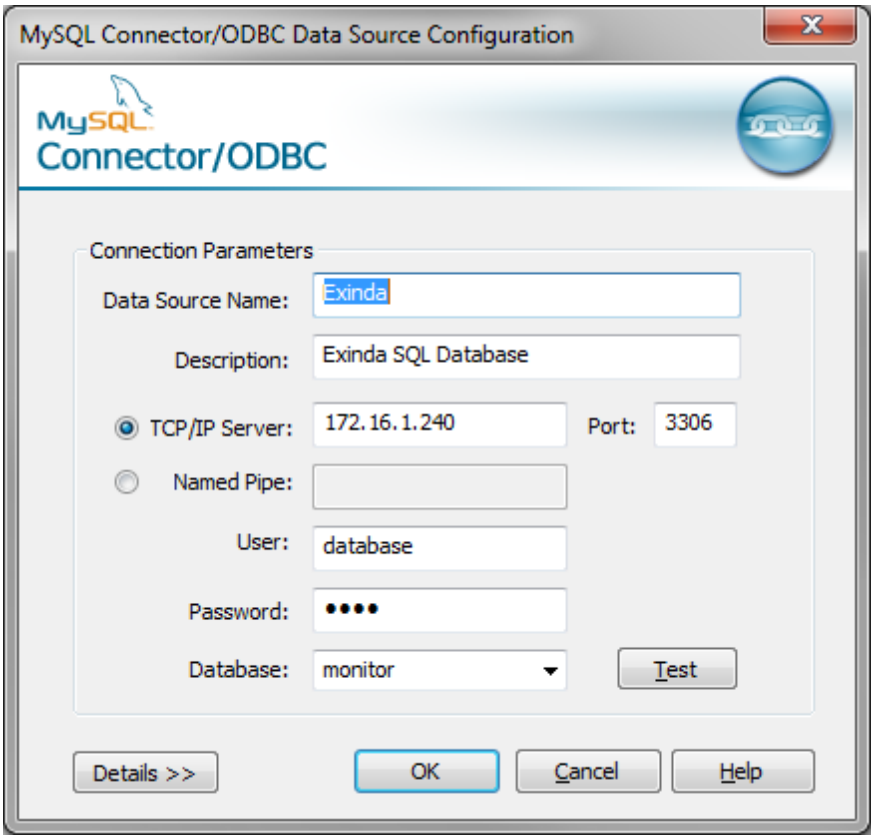


Select **MySQL ODBC Driver** and click **Finish**. You will be prompted to enter details about the SQL access using the form below:

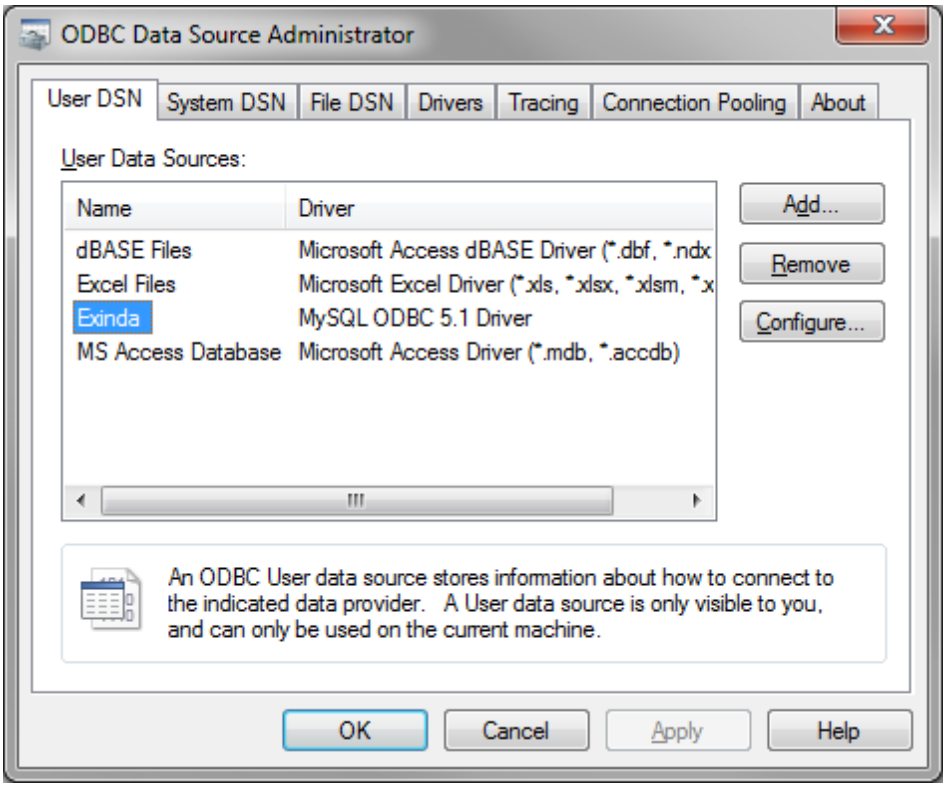


Data Source Name / Description	Enter a descriptive name for the DSN. E.g. 'Exinda SQL Database'.
Server	Enter the IP address of the Exinda appliance.
User	Enter the username you specified when enabling SQL access on the Exinda appliance.
Password	Enter the password you specified when enabling SQL access on the Exinda appliance.
Database	Once the above fields are configured, press the 'Test' button. If the connection attempt is successful, the 'Database' drop down will be populated with a list of available databases. Select 'monitor'.

Here is what a successful configuration looks like:



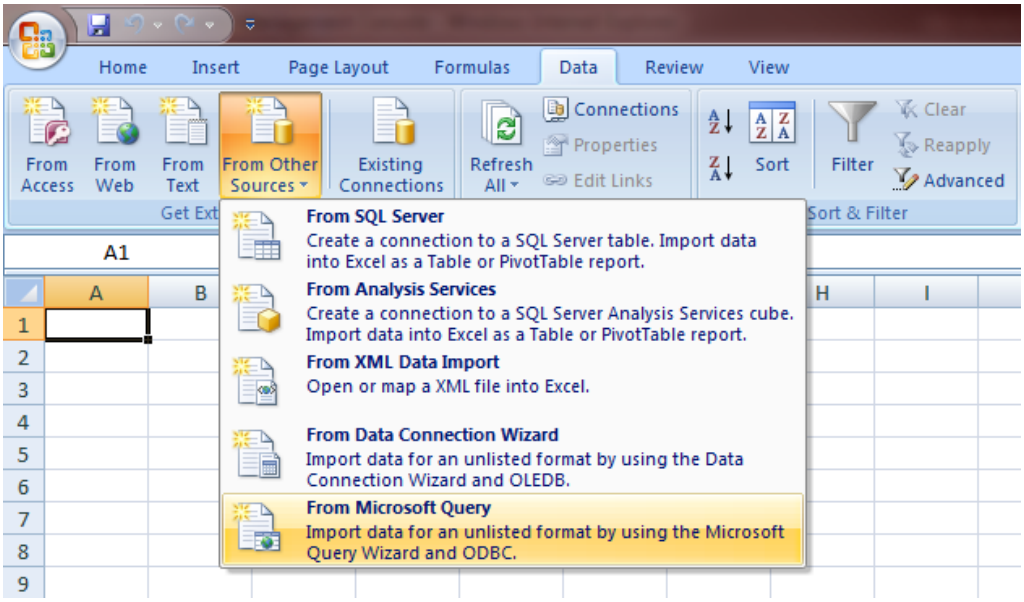
Click **OK**. This will add the 'Exinda SQL Database' to the list of available data sources that can be used by 3rd party applications on this client.



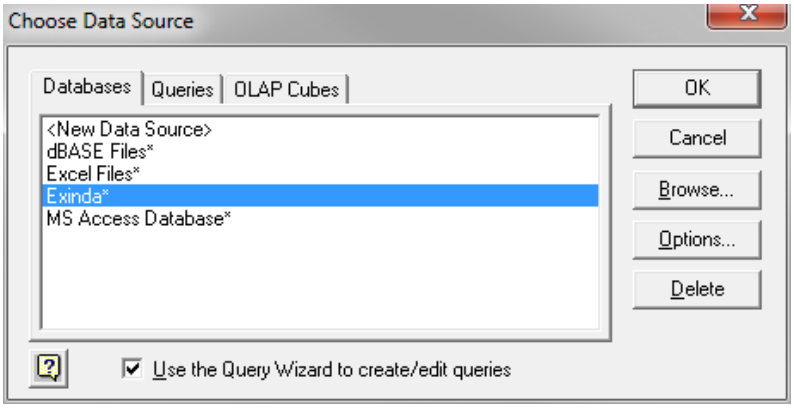
View SQL Access data in Microsoft Excel

You will need a 3rd party application that is capable of accessing data from ODBC data sources. For the purposes of this How to Guide, we will use Microsoft Excel as an example.

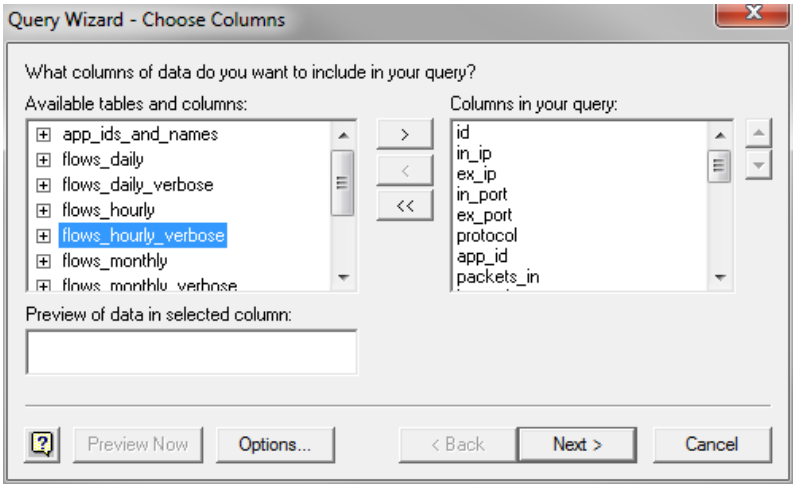
From the **Data** tab in Excel, select **From Other Sources > From Microsoft Query**.



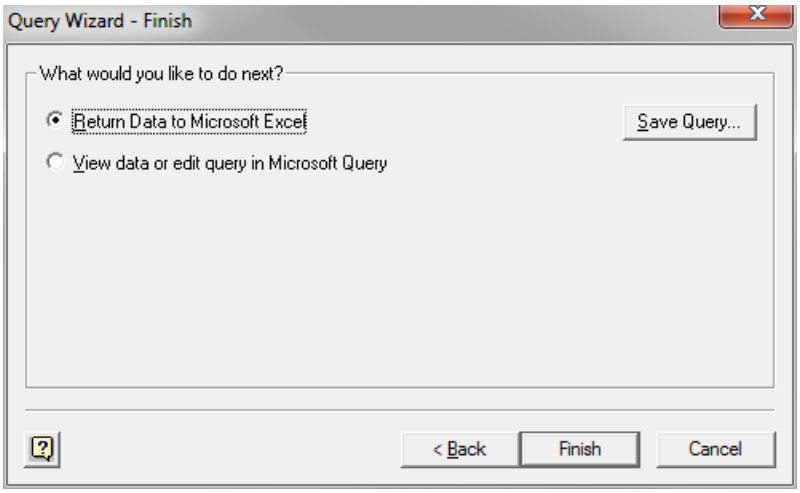
You will be presented with a dialog box that allows you to select the DSN you created in the previous chapter.



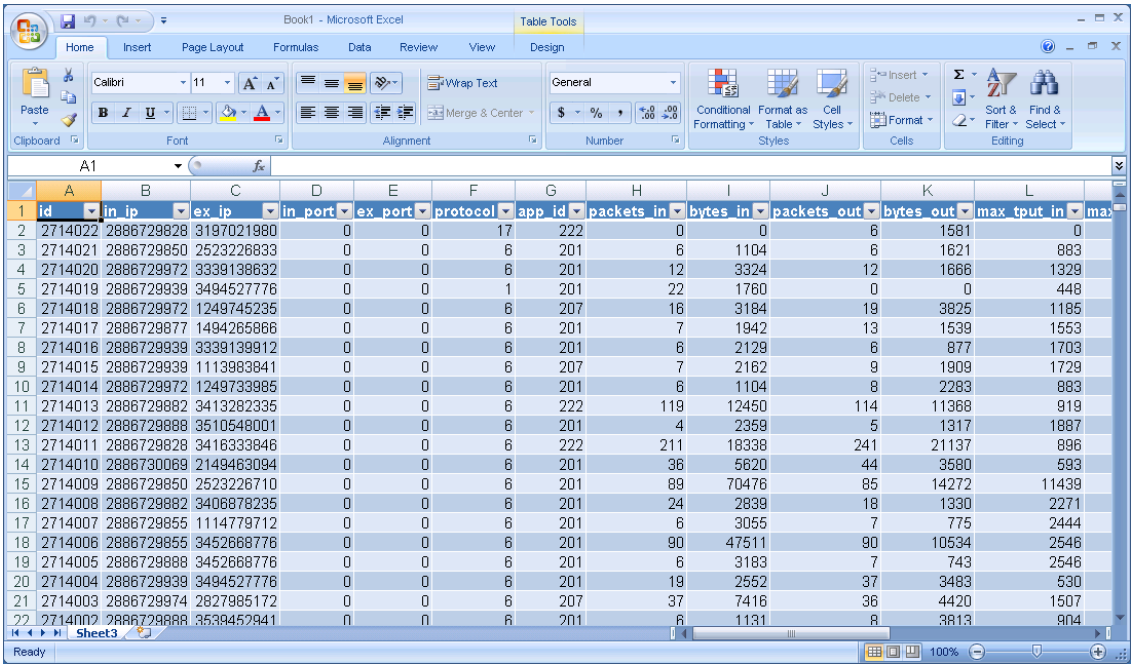
Select the **Exinda SQL Database** DSN. This will allow you to choose from the available tables and select the columns to query. Select a table and click the **>** button to move that table's fields into the list of columns to query.



Click through the wizard, optionally specifying columns to filter or sort by. Then click Finish to return the data to Excel.



The Exinda appliance will now be queried and the data will be returned to the Excel spreadsheet.



id	in_ip	ex_ip	in_port	ex_port	protocol	app_id	packets_in	bytes_in	packets_out	bytes_out	max_tput_in
2714022	2886729828	3197021980	0	0	17	222	0	0	6	1581	0
2714021	2886729850	2523226833	0	0	6	201	6	1104	6	1621	883
2714020	2886729972	3339138632	0	0	6	201	12	3324	12	1666	1329
2714019	2886729939	3494527776	0	0	1	201	22	1760	0	0	448
2714018	2886729972	1249745235	0	0	6	207	16	3184	19	3825	1185
2714017	2886729877	1494265866	0	0	6	201	7	1942	13	1539	1553
2714016	2886729939	3339139912	0	0	6	201	6	2129	6	877	1703
2714015	2886729939	1113983841	0	0	6	207	7	2162	9	1909	1729
2714014	2886729972	1249733985	0	0	6	201	6	1104	8	2283	883
2714013	2886729882	3413282335	0	0	6	222	119	12450	114	11368	919
2714012	2886729888	3510548001	0	0	6	201	4	2359	5	1317	1887
2714011	2886729828	3416333846	0	0	6	222	211	18338	241	21137	896
2714010	2886730069	2149463094	0	0	6	201	36	5620	44	3580	593
2714009	2886729850	2523226710	0	0	6	201	89	70476	85	14272	11439
2714008	2886729882	3406878235	0	0	6	201	24	2839	18	1330	2271
2714007	2886729855	1114779712	0	0	6	201	6	3055	7	775	2444
2714006	2886729855	3452668776	0	0	6	201	90	47511	90	10534	2546
2714005	2886729888	3452668776	0	0	6	201	6	3183	7	743	2546
2714004	2886729939	3494527776	0	0	6	201	19	2552	37	3483	530
2714003	2886729974	2827985172	0	0	6	207	37	7416	36	4420	1507
2714002	2886729888	3539452941	0	0	6	201	6	1131	8	3813	904

Chapter 2: SQL Schema

There are a total of 10 tables available for access via SQL.

Name	Description
flows_ hourly	Flow records at an hourly resolution, that is, information for each flow is stored hourly, on the hour.
flows_daily	Flow records at daily resolution, that is, information for each flow is stored daily, on the day at midnight.
flows_ monthly	Flow records at monthly resolution, that is, information for each flow is stored monthly, on the 1st day of the month at midnight.
urls_hourly	URL records for each flow record that contain 1 or more urls at hourly resolution, that is, information for each url is stored hourly, on the hour.
urls_daily	URL records for each flow record that contain 1 or more urls at daily resolution, that is, information for each url is stored daily, on the day at midnight.
urls_ monthly	URL records for each flow record that contain 1 or more urls at monthly resolution, that is, information for each url is stored monthly, on the 1st day of the month at midnight.
app_ids_ and_names	Application records. The record contains a name, id and a flag to indicate if the application has been deleted. Deleted applications are used when labeling historical data.
summary_ applications	Flow records summarized by application. Each record contains information gathered over a 5 minute period.
summary_ hosts_ex	Flow records summarized by external host. Each record contains information gathered over a 5 minute period.
summary_ hosts_in	Flow records summarized by internal host. Each record contains information gathered over a 5 minute period.

flows Table

The following table describes the schema of the flows_* SQL tables.

Field	Type	Description
id	unsigned 32-bit integer	A unique id that defines this record. This is the primary key.
in_ip	binary	A 16 byte (128 bit) representation of the internal IPv6 address (the IP

Field	Type	Description
	(128 bit)	address on the LAN side of the Exinda appliance) of the flow. IPv4 addresses are represented as IPv4 mapped format.
ex_ip	binary (128 bit)	A 16 byte (128 bit) representation of the external IPv6 address (the IP address on the WAN side of the Exinda appliance) of the flow. IPv4 addresses are represented as IPv4 mapped format.
in_port	unsigned 24-bit integer	The TCP or UDP port number on the internal side (the LAN side of the Exinda appliance) of the flow.[1]
ex_port	unsigned 24-bit integer	The TCP or UDP port number on the external side (the WAN side of the Exinda appliance) of the flow.[1]
protocol	unsigned 24-bit integer	The IANA assigned IP protocol number of the flow. See http://www.iana.org/assignments/protocol-numbers/ for more information.
app_id	unsigned 24-bit integer	The internal Exinda Application ID assigned to this flow. This represents Exinda's classification of the flow - 0 means unclassified.
packets_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) packets recorded for this flow over the sample period.
bytes_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) bytes recorded for this flow over the sample period.
packets_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) packets recorded for this flow over the sample period.
bytes_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) bytes recorded for this flow over the sample period.
max_tput_in	unsigned 64-bit integer	The maximum inbound (WAN -> LAN) throughput observed for this flow during the sample period.
max_tput_out	unsigned 64-bit integer	The maximum outbound (LAN -> WAN) throughput observed for this flow during the sample period.
intervals_in	unsigned 24-bit integer	The number of 10 second intervals there was inbound (WAN -> LAN) traffic observed for this flow during the sample period (bps).
intervals_	unsigned	The number of 10 second intervals there was outbound (LAN -> WAN) traffic

Field	Type	Description
out	24-bit integer	observed for this flow during the sample period (bps).
timestamp	unsigned 32-bit integer	A UNIX timestamp (number of seconds since epoch - 1st Jan 1970) that represents the start of the sample period.
in_ username	string	A string representation of the username that was assigned to the internal IP of this flow when it was created (if available).
ex_ username	string	A string representation of the username that was assigned to the external IP of this flow when it was created (if available).[1]
rtt	unsigned 32-bit integer	Round Trip Time in milliseconds. A measure if the time a packet takes to leave a device, cross a network and return.[2]
network_ delay	unsigned 32-bit integer	A normalized measure of the time taken for transaction data to traverse the network.[2]
network_ jitter	unsigned 32-bit integer	A normalized measure of the network_delay variability.[2]
server_ delay	unsigned 32-bit integer	A normalized measure of the time taken for a server to respond to a transaction request.[2]
bytes_ lost_in	unsigned 64-bit integer	The number of bytes lost due to retransmissions (WAN -> LAN).[2]
bytes_ lost_out	unsigned 64-bit integer	The number of bytes lost due to retransmissions (LAN -> WAN).[2]
aps	unsigned 64-bit integer	Application Performance Score. A measure of an applications performance on the network.[2]

[1] in_port and ex_port are only defined when the IP protocol is TCP (6) or UDP (17) and the Exinda was unable to classify the flow (so the app_id is 0).

[2] See the APS HowTO Guide for further information.

The flows_* tables are available as views that represent the binary IPv6 addresses in string format. The views tables are flows_*_verbose (e.g. flows_hourly_verbose). The fields are identical to the above except for the following:

Field	Type	Description
in_ip	string	A string representation of the internal address (the IP address on the LAN side of the Exinda appliance) of the flow. IPv4 mapped IPv6 addresses are represented as IPv4 dotted quad.
ex_ip	string	A string representation of the external address (the IP address on the WAN side of the Exinda appliance) of the flow. IPv4 mapped IPv6 addresses are represented as IPv4 dotted quad.

app_ids_and_names Table

The following table describes the schema of the app_ids_and_names SQL table.

Field	Type	Description
app_id	unsigned 24-bit integer	A unique id that defines the Application. This is the primary key.
app_name	string	The Application name (e.g HTTP, Hotmail)
deleted_flag	unsigned 8-bit integer	A flag indicating if the Application has been deleted from the appliance (0 = no, 1 = yes)

urls Table

The following table describes the schema of the urls_* SQL tables.

Field	Type	Description
id	unsigned 32-bit integer	This id references an id in the corresponding parent flows_* table. There can be multiple url records referencing the same flow id, so this field is not unique.
url	string	The URL (host) extracted from the HTTP header of the parent flow.
packets_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) packets recorded for this URL over the sample period.
bytes_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) bytes recorded for this URL over the sample period.
packets_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) packets recorded for this URL over the sample period.
bytes_	unsigned	The number of outbound (LAN -> WAN) bytes recorded for this URL over the

Field	Type	Description
out	64-bit integer	sample period.
max_ tput_in	unsigned 64-bit integer	The maximum inbound (WAN -> LAN) throughput observed for this URL during the sample period.
max_ tput_out	unsigned 64-bit integer	The maximum outbound (LAN -> WAN) throughput observed for this URL during the sample period.
intervals_ in	unsigned 16-bit integer	The number of 10 second intervals there was inbound (WAN -> LAN) traffic observed for this URL during the sample period.
intervals_ out	unsigned 16-bit integer	The number of 10 second intervals there was outbound (LAN -> WAN) traffic observed for this URL during the sample period.

Note id's are only consistent across the same sample periods. For example, id's in the urls_ hourly table only reference id's in the flows_hourly table.

summary_applications Table

The summary_application table summarizes the aggregated data from the Exinda. The following table describes the schema of the summary_applications SQL table.

Field	Type	Description
in_port	unsigned 24-bit integer	The TCP or UDP port number on the internal side (the LAN side of the Exinda appliance)[1]
ex_port	unsigned 24-bit integer	The TCP or UDP port number on the external side (the WAN side of the Exinda appliance)[1]
protocol	unsigned 24-bit integer	The IANA assigned IP protocol number of the flow. See http://www.iana.org/assignments/protocol-numbers/ for more information.
app_id	unsigned 24-bit integer	The internal Exinda Application ID assigned to this flow. This represents Exinda's classification of the flow. A zero value should be interpreted as unclassified.
bytes_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) bytes recorded for this flow over the sample period.

Field	Type	Description
bytes_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) bytes recorded for this flow over the sample period.
packets_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) packets recorded for this flow over the sample period.
packets_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) packets recorded for this flow over the sample period.
intervals_in	unsigned 24-bit integer	The number of 10 second intervals there was inbound (WAN -> LAN) traffic observed for this flow during the sample period.
intervals_out	unsigned 24-bit integer	The number of 10 second intervals there was outbound (LAN -> WAN) traffic observed for this flow during the sample period.
timestamp	unsigned 32-bit integer	A UNIX timestamp (number of seconds since epoch - 1st Jan 1970) that represents the start of the sample period.
max_tput_in	unsigned 64-bit integer	The maximum inbound (WAN -> LAN) throughput observed for this flow during the sample period (bps).
max_tput_out	unsigned 64-bit integer	The maximum outbound (LAN -> WAN) throughput observed for this flow during the sample period (bps).
rtt	unsigned 32-bit integer	Round Trip Time in milliseconds. A measure of the time a packet takes to leave a device, cross a network and return.[2]
network_delay	unsigned 32-bit integer	A normalized measure of the time taken for transaction data to traverse the network.[2]
network_jitter	unsigned 32-bit integer	A normalized measure of the network_delay variability.[2]
server_delay	unsigned 32-bit integer	A normalized measure of the time taken for a server to respond to a transaction request.[2]
bytes_lost_in	unsigned 64-bit integer	The number of bytes lost due to retransmissions (WAN -> LAN).[2]

Field	Type	Description
bytes_lost_out	unsigned 64-bit integer	The number of bytes lost due to retransmissions (LAN -> WAN).[2]

[1] in_port and ex_port are only defined when the IP protocol is TCP (6) or UDP (17) and the Exinda was unable to classify the flow (so the app_id is 0).

[2] See the APS How To Guide for further information.

summary_hosts Table

The following table describes the schema of the summary_hosts_in and summary_hosts_ex SQL tables. The table fields are identical apart from the ip field - this field represent the IPv4 or IPv6 address of an internal host (summary_hosts_in) or an external host (summary_hosts_ex).

A host is internal if it is on the LAN side of the appliance and external when on the WAN side.

Field	Type	Description
ip	binary string	A string representation of the internal or external IPv4 or IPv6 address of the host.
bytes_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) bytes recorded for this flow over the sample period.
bytes_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) bytes recorded for this flow over the sample period.
packets_in	unsigned 64-bit integer	The number of inbound (WAN -> LAN) packets recorded for this flow over the sample period.
packets_out	unsigned 64-bit integer	The number of outbound (LAN -> WAN) packets recorded for this flow over the sample period.
intervals_in	unsigned 24-bit integer	The number of 10 second intervals there was inbound (WAN -> LAN) traffic observed for this flow during the sample period (bps).
intervals_out	unsigned 24-bit integer	The number of 10 second intervals there was outbound (LAN -> WAN) traffic observed for this flow during the sample period (bps).
timestamp	unsigned 32-bit integer	A UNIX timestamp (number of seconds since epoch - 1st Jan 1970) that represents the start of the sample period.

Field	Type	Description
max_tput_in	unsigned 64-bit integer	The maximum inbound (WAN -> LAN) throughput observed for this flow during the sample period.
max_tput_out	unsigned 64-bit integer	The maximum outbound (LAN -> WAN) throughput observed for this flow during the sample period.
rtt	unsigned 32-bit integer	Round Trip Time in milliseconds. A measure if the time a packet takes to leave a device, cross a network and return.[1]
network_delay	unsigned 32-bit integer	A normalized measure of the time taken for transaction data to traverse the network.[1]
network_jitter	unsigned 32-bit integer	A normalized measure of the network_delay variability.[1]
server_delay	unsigned 32-bit integer	A normalized measure of the time taken for a server to respond to a transaction request.[1]
bytes_lost_in	unsigned 64-bit integer	The number of bytes lost due to retransmissions (WAN -> LAN).[1]
bytes_lost_out	unsigned 64-bit integer	The number of bytes lost due to retransmissions (LAN -> WAN).[1]

[1] See the APS How To Guide for further information.