IceWarp Unified Communications

Log Analyzer – Viewer Guide

Version 12

Published on 3/6/2017

Contents

Log Analyzer – Viewer

IceWarp Log Analyzer (ILA) is a statistical and logical analysis tool for log files generated by IceWarp Server.

Introduction

IceWarp Log Analyzer processes log files and organizes information in records stored in an SQL database. The logged activity can be monitored using the Log Viewer (ILA) application, allowing the system administrator to search for specific events for troubleshooting purposes or simply to improve system efficiency.

Special Thanks

Flávio Lucarelli of LucaNet Sistemas Ltda. (Brasil IceWarp partner)
His suggestions and his help were invaluable.
Thank you very much Flávio.

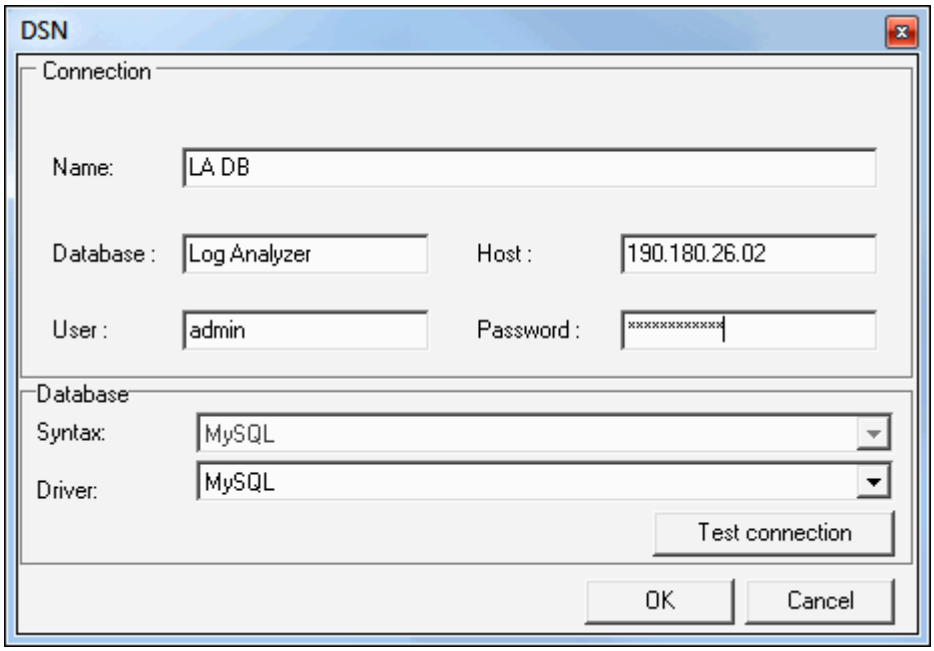
Getting Started

After you launched ILA, if you are in remote mode, you need to setup its initial configuration. ILA uses an external database to operate, so you need to configure the connection to the database.

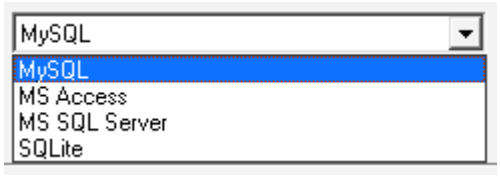
Databases supported are MySQL, MS SQL Server and MS Access so you need to choose between these databases.

If you are using MySQL or MS SQL Server, you need to create the database on you server and set the rights to let ILA access the database.

Now, you need to configure the database connection.



Select the database you want to use:



and click the ***Built-in DSN wizard*** button.

A window opens where you have to type in the database connection parameters.

Click the ***Test*** button to verify if the connection can be established.

Click ***OK*** to close and confirm the parameters typed.

Click the ***Create tables*** button in order to create tables that ILA needs to store log data.

If you experience any problem during this step, it may be that your database rights are not enough to create tables, check with your database administrator for the solution.

If you use MySQL, read the **MySQL Troubleshooting** chapter.

*NOTE: You can use wildcards ***** or **%** in the fields where you enter strings to (e.g. FROM IP, FROM username, FROM domain, TO username, TO account, ...).*

*For example, in the **From domain** field you can use icewarp.* – you will see logs for all icewarp domains (icewarp.com, icewarp.net, etc.).*

Log Analyzer Configuration

Quick installation

1. Right after installation, if you tick the ***Active*** box (within the **Log Analyzer – General** tab), the default MS Access database will be used.
2. On the server, you can start importing SMTP logs using the ***Import Now*** button.

   NOTE: The console has to remain open during the import.
3. In Log Analyzer, check logs – the result of the import process.
4. Start the Viewer. On the server, a default DSN will be created with the same settings of the importer (the configuration is read by IceWarp API).

NOTE: The "default" connection is created only when Viewer is started without a defined connection and on the server that runs the importer.

Remote Viewer Usage

You do not have to create any system or other DSN to use IceWarp Log Analyzer, the viewer uses native drivers for all the supported databases.

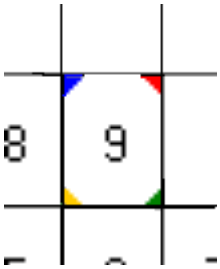
Double-click the ***Database Connection – New*** tree item and set the parameters for the database. You can check the connection by clicking the ***Test connection*** button.

To view the complete session, you also have to copy the raw log files from the remote machine to the local one. The default setting is to search the raw log files in the ***logs*** directory where Viewer is.

Import Log Files

In the **Calendar** tab, you can see a whole year calendar in which some days have small colored corner with different colors.

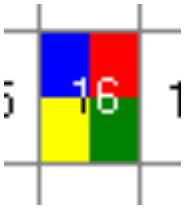
Another way how to import logs is via the command line.



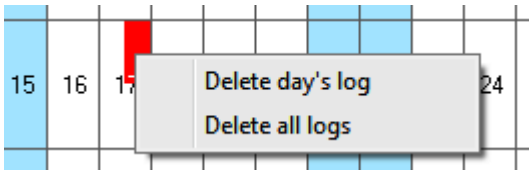
Colored corners mean that log files for the displayed day exist in the base log directory.
Colors are different for different log file types:

- BLUE means SMTP log files;
- RED means POP3 log files;
- YELLOW means ANTI-VIRUS log files;
- GREEN means ANTI-SPAM log files;
- VIOLET means IMAP log files;

After log files are imported the colors change and occupy the entire area for that day (or a square part):



Right clicking a day, you will get a pop-up menu that lets you delete either logs of the selected day or all of them.



Single SMTP Logs

To import a single SMTP log, double-click the ***Database connections – <internal> – Import*** left pane tree item. The usual **Open** dialog allows you to browse for a single SMTP log file.

Import of Current Day Logs

To import logs for a current day, you can create a batch file with the ***-dtoday*** switch.

NOTE: If a single SMTP session that spans two days occurs (e. g. starts at 11:58 PM and finishes at 00:03 AM the next day), ILA will not show it as one single session. Only the part of log from the respective day will be shown.

Import of Logs from Date Range – Command Line Use

Another way how to import logs is via the command line. To import logs for some date range, use the following command:

mlaimp -dYYYYMMDD-YYYYMMDD

Example:

To import all log files for August, use: ***mlaimp -d20120801-20120831***

Also, to show importer usage, enter the following command: ***mlaimp -?***

IP Statistics

Using **IP statistics**, you can obtain information about the traffic originated from or destined to specific IP addresses.

For each remote IP address, the following information is displayed:

Count	Number of messages processed by the IceWarp Server.
Size	The total size in MB of the messages.
Duration	The total duration of all the sessions expressed as hh:mm:ss.
Failed	The number of failed messages.
Succeeded	The number of successfully delivered messages.

Using **Common Filters**, you can focus on a part of the entire data that was logged.

Domain Statistics

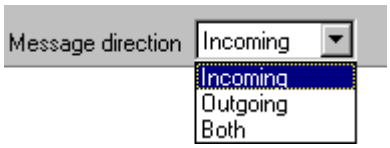
Domain statistics window returns information about the traffic originated from or addressed to local domains.

For each domain the following information are displayed:

Count	The number of mails processed by IceWarp Server.
Size	The size in MB of the data transferred.
Duration	The sum of the duration of all the sessions, expressed as hh:mm:ss.
Failed	The number of failed messages.
Succeeded	The number of successfully delivered messages.

Using **Common Filters**, you can focus on a part of the entire data that was logged.

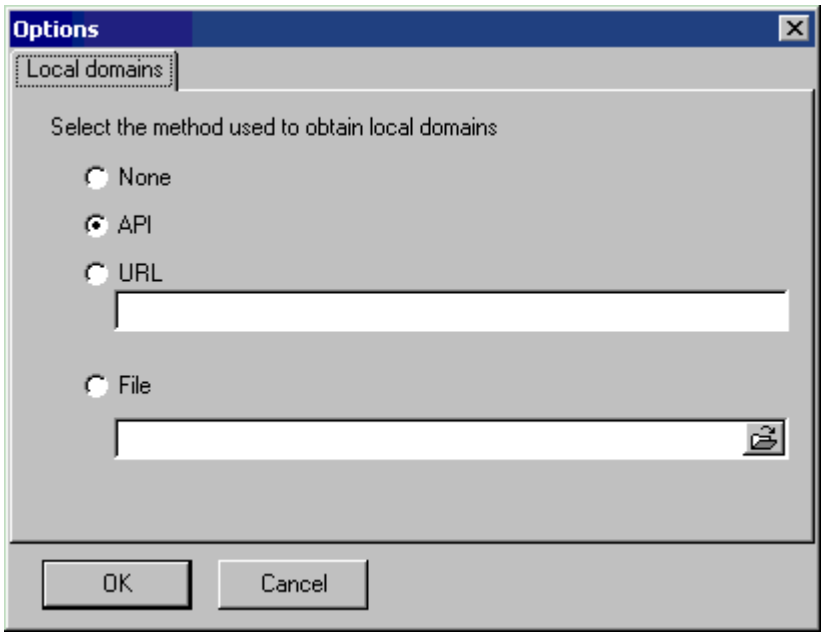
You can filter results using the message direction selector,



which limits the report to incoming, outgoing messages or both.

To filter a local domain only, use the ***Only local domains*** check box.

To use these options, you must configure the local domain list from IceWarp Server. This list can be retrieved in many ways. To configure how get local domains list use the option window:



The options are:

API	If ILA is installed on the same machine as IceWarp Server, you can use IceWarp API to get local domains list. It is the simplest way.
URL	A web page that returns a page with a list of domains. Useful when ILA is not installed on the same machine as IceWarp Server, the page can be served using IceWarp integrated Web Server.
File	A simple ASCII text file, with one domain listed per row. Useful if none of the previous ways are feasible. IceWarp Server provides a tool to export domain list, look for **tool.exe** in IceWarp Server Help. Usage: `tool.exe export domain * > file_list.txt`

User Statistics

User statistics window returns information about traffic originated from or addressed to local accounts.

For each user the information returned is:

Count	The number of mails processed by the IceWarp Server.
Size	The size in MB of the data transferred.
Duration	The sum of the duration of all sessions expressed in hh:mm:ss.
Failed	The number of failed messages.
Succeeded	The number of successfully delivered messages.

Using **Common Filters** you can focus on a part of the entire data that was logged.

Global

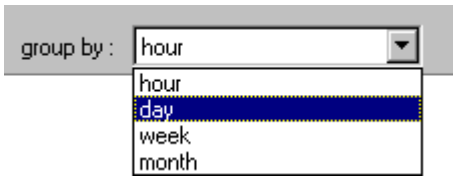
Global statistics display how many messages were successfully delivered, how many messages were blocked and why.

Messages are classified as:

OK	The message was delivered correctly.
DNSBL	The session was refused due to a "DNS Black List" filter. The sender's IP address has been banned due to spamming or other unwanted activities.
ANA	The message was refused because the sender has no access permission (Access Not Allowed).
AS	The message was refused by the Anti-Spam.
AV	The message was detected by the Anti-Virus.
DBF	The message was "Deleted By Filter". This is usually a Content Filter.
SDME	The message was refused because the sender's domain doesn't exist (Sender's Domain Must Exist).
SCAN	An incoming connection has been established but no message delivery was attempted. This behaviour is typical of port and service scan tools.
TARP	The originating IP address was tarpitted by IceWarp Server, thus the delivery session was rejected. Tarpitting is now Intrusion Prevention.
WDNR	The message was refused because relaying to the final recipient was not allowed (We Do Not Relay).
UNK	The message was refused because the recipient address doesn't exist (User Unknown).
CNC	A client session failed because IceWarp Server couldn't connect to the remote SMTP server (Could Not Connect).
ERROR	The message wasn't delivered due to some unspecified error.
CA	The message was accepted and forwarded to a catch-all address (Catch All account).
INCPLT	The session is incomplete.
GRLST	The message was refused by Gray Listing.

The table reports the number of sessions or messages succeeded and those refused for each reason.

You can obtain a report per hour, day, week or month selecting the ***Group by*** selector.



Using **Common Filters**, you can focus on a part of the entire data that was logged.

After the report has been generated, you can easily focus your attention on relevant situations using the highlight threshold option. Values higher than the threshold compared to the total ***Processed*** are highlighted.

The following picture shows how SCAN and UNK activities are relevant on the server being analyzed.

Hour	Processed	Succeeded	ANA	AV	DBF	DNSBL	SDME	TARP	UNK	SCAN	WDNR	CNC	ERROR
2005-12-18 00:00:00	1770	258	156	18	6	432	6	30	306	498	0	0	0
2005-12-18 01:00:00	1332	210	4	0	6	310	0	20	292	474	0	0	4
2005-12-18 02:00:00	1016	207	10	4	16	167	8	7	330	228	0	0	0
2005-12-18 03:00:00	702	78	15	3	3	165	6	0	171	252	0	0	0
2005-12-18 04:00:00	711	102	12	9	0	117	6	12	183	240	0	0	0
2005-12-18 05:00:00	753	168	0	0	0	147	9	15	204	201	0	0	0
2005-12-18 06:00:00	354	48	17	2	3	73	4	2	66	125	0	0	0
2005-12-18 07:00:00	179	57	0	0	1	33	0	2	34	51	0	0	0

Using the percentage button "%", you can switch values so they are specified in percentage in relation to the processed messages value. This is useful to estimate the importance of each value/item.

Mail Search

This powerful search tool can be used for several tasks, like:

- search for a specific message and see if it was accepted or the reason it was rejected for
- detailed analysis of incoming and outgoing traffic per domain/user
- search for message delivery session matching specific conditions

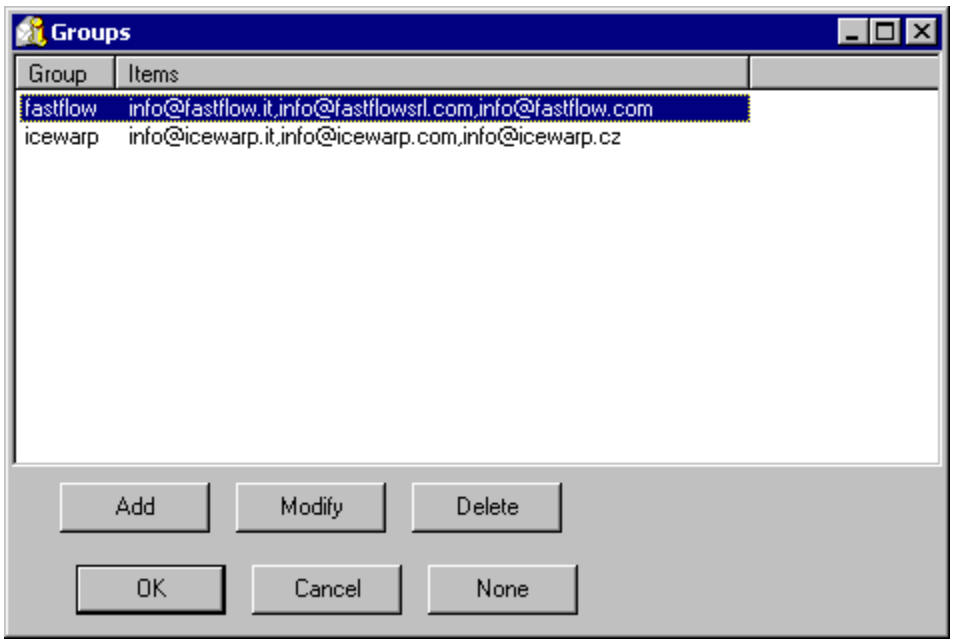
In addition to the standard **Common Filters** you may specify a filter on:

From account	The alias of the "MAIL FROM" address
From domain	The domain of the "MAIL FROM" address
To account	The alias of the "RCPT TO" address
To domain	The domain of the "RCPT TO" address

Using **Common Filters**, you can focus on a part of the entire data that was logged.

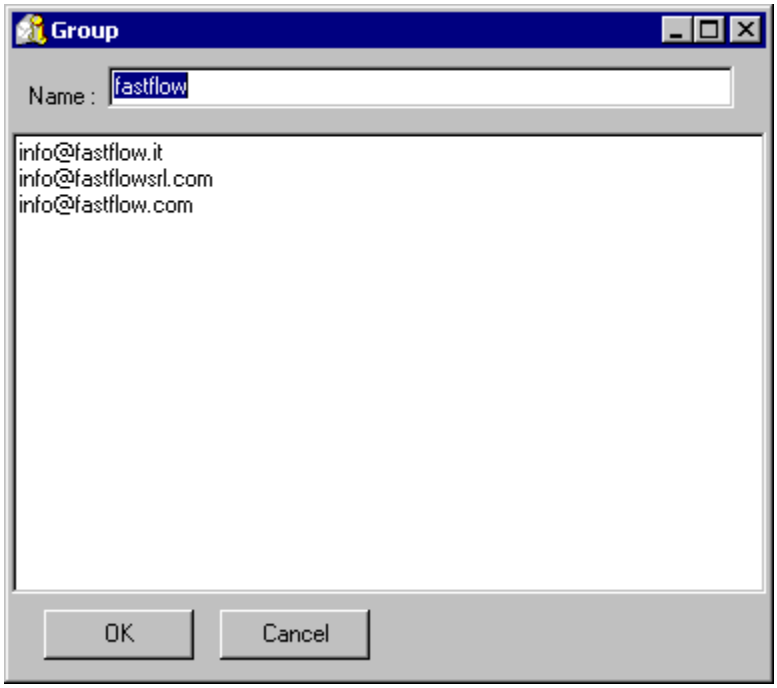
Using button list  you can list all the available from/to accounts or from/to domains and select the item you need.

In order to filter on more than one domain or account you can create groups of values. Clicking on the groups button  the groups manager is displayed:



Here you can add, delete or modify groups.

A group is a list of mail addresses used to filter log data.



You can filter on the result of the session.

You can read the meaning of acronyms in the **Global Statistics** section of this guide.

Searching for Messages Sent via Mailing List

To perform this search, follow these steps:

1. Double-click the ***SMTP log search*** node.
2. Enter the mailing list address to the ***To:*** field, perform your search.
3. Copy the ***Message ID*** from the appropriate column and paste it to the ***Message ID*** field.
4. Delete the address from the ***To:*** field and perform your search again.

Direct Search Method

To search, you have to:

1. Select ***Direct search*** in the left panel.
2. Select the log file using the "..." button.
3. Insert the search term and press the button at the right of the search string, the search string is not a regex and you cannot use "*" or other special characters.

   Examples of valid search strings are:

   "***" – to search for all sessions in the log, since "***" is the summary line at the end of each session;

   Client session – to search for all the client sessions;

   @icewarp.com.br – to search for all sessions that contain "@icewarp.com.br"
4. You can now refine your search using the ***From*** and ***To*** filters. When you want to filter the previous search, you have to press the button with the play button on the left.

If you right-click a row, you can search for ***Message ID*** and see the whole processing of this message. The search time is proportional to the number of results. (For example with a 50 MB log file with ~ 8000 sessions, to get the result took less than 200 ms.) If you right-click a session, you will find the ***Search MessageID*** function.

There is also a contextual menu in the part where you see the whole session; you can select a string in the session and if it can be decoded using ***base64***, it will be shown as a hint when you stop moving the mouse.

Duration Statistics

The **Duration** section gives detailed information about the time required to process messages, classified and grouped by the result of the corresponding sessions.

Times are expressed as hh:mm:ss.

Statistics displayed are:

MinDuration	The minimum processing time for a message of this class
MaxDuration	The maximum processing time for a message of this class
AvgDuration	The average processing time for a message of this class
SumDuration	The total processing time for this class
SumSize	The total amount of data transferred during all the sessions

These statistics help understanding how the overall load is distributed and whether IceWarp Server's filters and security systems are efficient or need further tuning.

Using **Common Filters**, you can focus on a part of the entire data that was logged.

Custom Search

If you are looking for specific problems and the default statistics do not fit your needs, you can access data stored in ILA's database tables and write your own SQL query to extract any kind of information.

Special parameters can be included in the SQL syntax to facilitate the insertion of filter values. Parameters provide you with specific input fields.

Parameter syntax:

:[`parameter_name[:default_value[:parameter_type[:parameter_format]]]`**]**

Example 1:

```
SELECT * FROM smtp WHERE lg_FromDomain=:[Domain]
```

in the above example the parameter "Domain" replaces a "From Domain" static value.

Example 2:

```
SELECT * FROM smtp WHERE lg_FromDomain=:[Domain:icewarp.it]
```

in the above example the parameter "Domain" replaces a "From Domain" static value and sets the default value to "icewarp.it".

Example 3:

```
SELECT * FROM smtp WHERE lg_Duration>:[Min Duration:100:integer]
```

in the above example the parameter "Min Duration" replaces a "Duration" static value and sets the default value to "100". It declares the parameter as integer type, so you get an integer value edit box.

Example 4:

```
SELECT * FROM smtp WHERE lg_Date>':[Since:07/06/2005:Date]'
```

in the above example the parameter "Since" replaces a "Date" static value and sets the default value to "07/06/2005". It declares the parameter as date type, so you get a calendar edit box.

Example 5:

```
SELECT * FROM smtp WHERE lg_Date>':[Since:07/06/2005:Date:yyyy-mm-dd]'
```

in the above example the parameter "Since" replaces a "Date" static value and sets the default value to "07/06/2005". It declares the parameter as date type, so you get a calendar edit box. The parameter value used in SQL commands is formatted as "yyyy-mm-dd" to match specific database requirements.

Database Tables and Fields

ILA Tables

Log data is stored in database tables with the following structure:

SMTP Table

lg_AI recordID	The record ID
lg_ATRN	The domain name for which the ATRN command is executed
lg_ATRN_res	The result of the ATRN command execution: **"N"** not an ATRN session; **"S"** there were messages for the domain; **"F"** there wasn't any message for the domain;
lg_AUTH	The result of the AUTH command execution: **"N"** no authentication took place; **"S"** user authenticated successfully; **"F"** authentication failed;
lg_AV	Antivirus response if delivered message had infected content.
lg_AccessNotAllowed	**"Y"** the message was stopped by a black list or a helo filter; **"N"** this condition didn't apply;
lg_ClientSession	**"Y"** the session was a client session; **"N"** the session was a server session;
lg_DNSBL	If present, this is the hostname of the DNSBL system that listed the sender's IP address.
lg_Date	The date of the session.
lg_DeletedByFilter	If present, this is the name of the filter which rejected the message.
lg_DomainSenderMustExist	**"Y"**, the message was rejected because the sender domain doesn't exist.
lg_Duration	The duration of the session in seconds.
lg_ETRN	The domain name for which the ETRN command is executed.
lg_Error	"**OK**" no error occurred; otherwise can be one of the following values **"TARP"**,**"ANA"**,**"UNK"**,**"SDME"**,**"SCAN"**,**"AV"**,**"DNSBL"**,**"DBF"**,**"WDNR"**,**"ERROR"**.
lg_FromAccount	Sender's alias.
lg_FromDomain	Sender's domain.
lg_FromIP	The IP address of the remote system.
lg_Helo	If present, this is the HELO value submitted to the server.
lg_Incomplete	**"Y"** the session wasn't completed;

	"N" the session was completed correctly.
lg_Log	Raw session data, compressed with the ZLib algorithm.
lg_LogRows	Raw session data line count.
lg_MessageID	The Message ID, if any message has been accepted.
lg_Relay	**"N"** the message was not to be relayed or relaying was denied; **"Y"** the message was correctly relayed.
lg_Scan	**"PROT"** the remote system only asked for server capabilities and disconnected. **"PORT"** no actual session took place, the remote system merely connected and disconnected. **"N"** the session had a normal behavior.
lg_Server	The Server ID.
lg_Size	The size of the mail in bytes.
lg_TLS	The response to a TLS command: **"N"** no TLS was requested; **"S"** the TLS command completed successfully; **"N"** the TLS command reported an error.
lg_TS	The time-stamp of log processed by ILA
lg_Tarpitting	**"Y"** the remote IP address was rejected by the Tarpitting system; **"N"** Tarpitting was not triggered or was not active.
lg_ThreadID	The Thread ID of the connection.
lg_Time	The time the connection started at.
lg_ToAccount	Recipient's alias.
lg_ToDomain	Recipient's domain.
lg_UserUnknown	**"Y"** destination address doesn't exist on the server; **"N"** the destination address was accepted by the server.

POP3 Table

pop_AI	The record ID.
pop_Server	The Server ID.
pop_ThreadID	The Thread ID of the connection.
pop_FromIP	The IP address of the remote system.
pop_Date	The date of the session.
pop_Time	The time the connection started at.
pop_Duration	The duration of the session in seconds.
pop_RETR_Count	Number of messages retrieved from the server.

pop_RETR_Size	Total size of messages retrieved from the server.
pop_DELE_Count	Number of messages deleted.
pop_AUTH	The result of the AUTH command execution: **"N"** the command was not submitted; **"S"** authentication successful; **"F"** authentication failed.
pop_Account	Mailbox username.
pop_Password	Mailbox password.
pop_Log	Raw session data, compressed with ZLib algorithm.
pop_LogRows	Raw session data line count.
pop_MsgSize	The size of messages contained in the mailbox.
pop_MsgCount	The number of messages contained in the mailbox.
pop_Error	The error, in case of failure.
pop_ClientSession	**"Y"** a client session (remote account); **"N"** a normal POP3 session;

Antispam Table

as_AI	The record ID
as_Server	The server ID.
as_ThreadID	The Thread ID of the connection.
as_FromIP	The IP address of the remote system.
as_FromAccount	Sender's alias.
as_FromDomain	Sender's domain.
as_Date	The date of the session.
as_Time	The time the session started at.
as_MessageID	The Message ID.
as_Log	Raw session data, compressed with ZLib algorithm.
as_LogRows	Raw session data line count.
as_ToAccount	Recipient's alias.
as_ToDomain	Recipient's domain.
as_Score	The overall spam score.

as_Action	The action performed by the server.
as_RSBody	A bitmask of the following values: Parts = 0x0001 External = 0x0002 NoText = 0x0004 Script = 0x0008 Differ = 0x0010 NoBodyNoSubject = 0x0020 Filters = 0x0040
as_RSByPass	A bitmask of the following values: License = 0x0001 WhiteList = 0x0002 Trusted = 0x0004 Outgoing = 0x0008 Size = 0x0010 Bypass = 0x0020 NoUser = 0x0040 Mode = 0x0080
as_RSCharset	A bitmask of the following values: CharsetFilter = 0x0001 CharsetMissing = 0x0002
as_RSBayes	Bayesian filter score.
as_RSSpamAssassin	SpamAssassin score.
as_RSBW	**"Y"** black & white list has been applied; **"N"** no black & white list was involved;
as_RSContentFilter	**"Y"** a content filter has been applied; **"N"** no content filter was involved;
as_RSStaticFilter	**"Y"** a static filter has affected the action; **"N"** none static filter was involved;
as_RSChallengeResponse	**"Y"** challenge/response has been applied; **"N"** no challenge/response was involved;

Antivirus Table

av_AI	The record ID.
av_Server	The server ID.
av_ThreadID	The Thread ID of the connection.
av_FromIP	The IP address of the remote system.
av_FromAccount	Sender's alias.
av_FromDomain	Sender's domain.
av_Date	The date of the session.
av_Time	The time the session started at.

av_MessageID	The Message ID.
av_Log	Raw session data, compressed with ZLib algorithm.
av_LogRows	Raw session data line count.
av_ToAccount	Recipient's alias.
av_ToDomain	Recipient's name.
av_Virusname	The name of the virus found.
av_Filename	The name of the file containing the virus.

MySQL Troubleshooting for ODBC Connections

Configuring MySQL External DNS

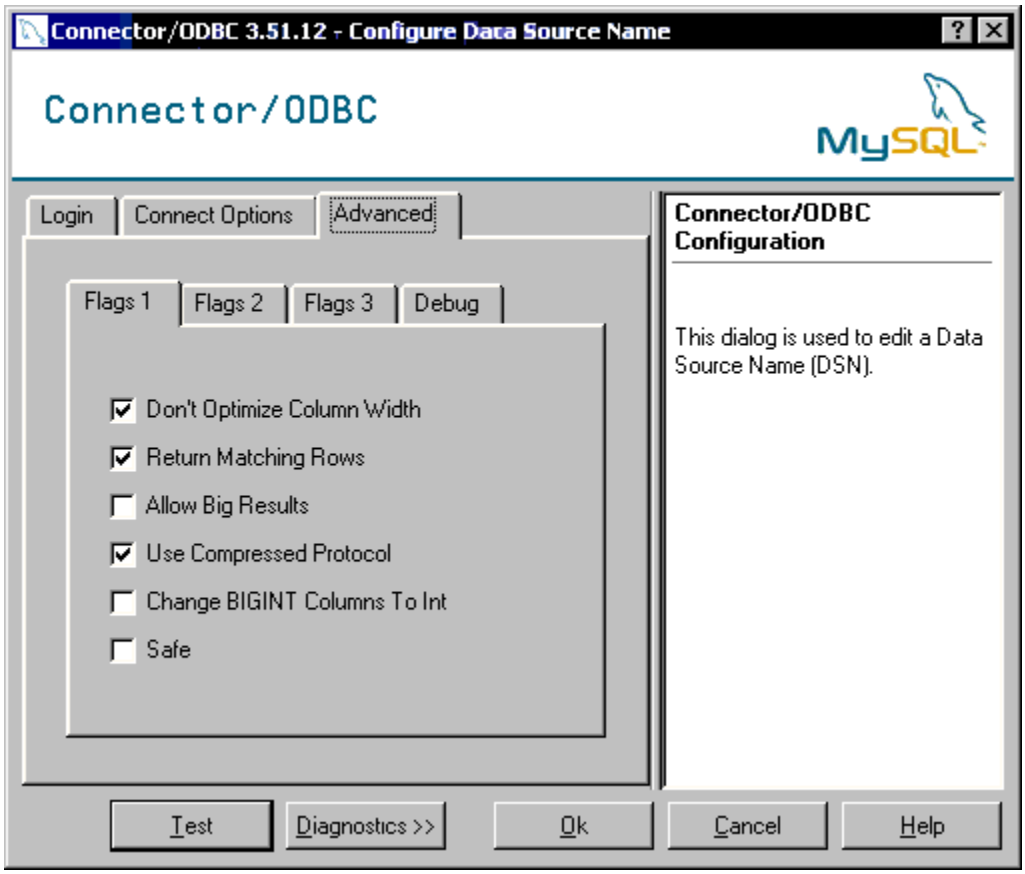
If you do not use the internal DNS configuration (it is recommended to use it), it is important to fine tune your ODBC driver's option.

ILA has an editor to help you configure ILA import utility.

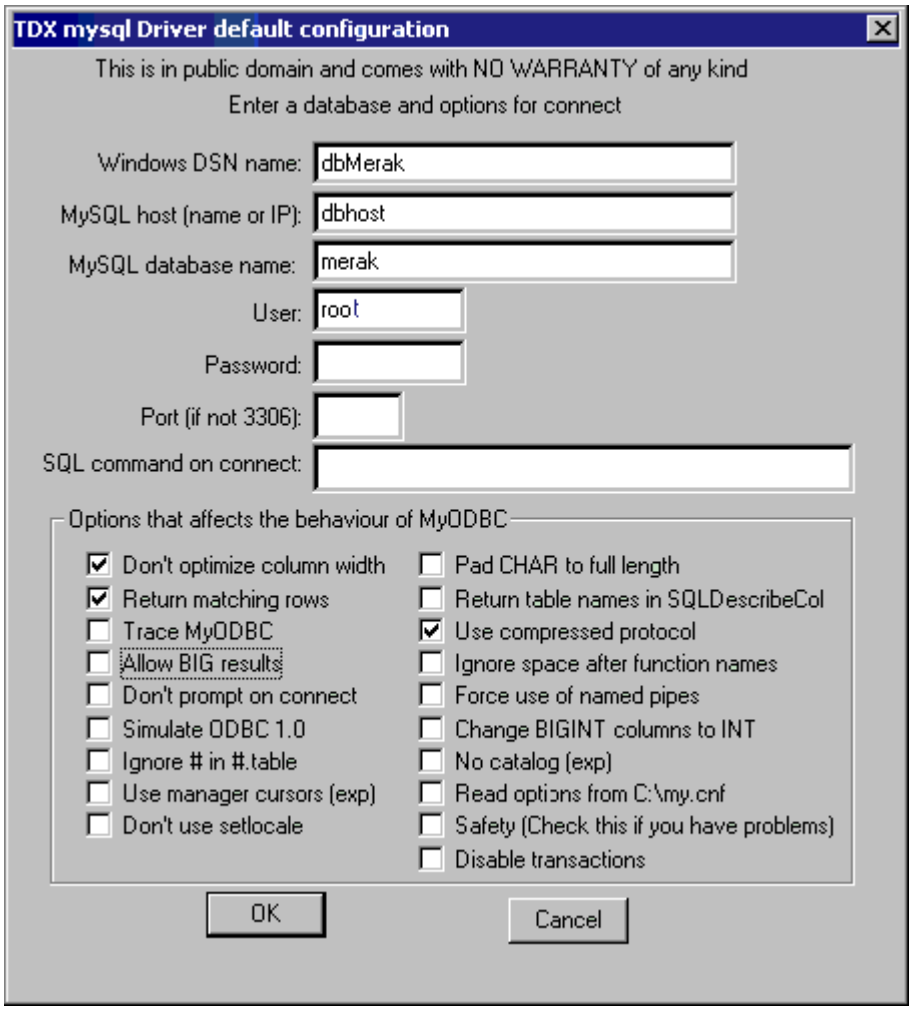
The correct configuration options for a DNS that accesses a MySQL is as follows:

Don't optimize column width
Return matching rows
Use compressed protocol

If you use MySQL ODBC driver 3.51.XX your configuration looks like the next image.



If you use MySQL ODBC driver 2.50.XX your configuration looks like the next image.



MySQL Server Version 5.00 or Newer

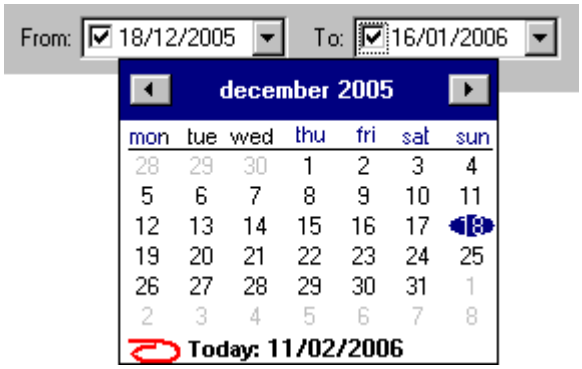
If your MySQL server version is 5.00 or newer, you have to use MySQL ODBC Driver 3.51.12 or newer to let ILA to work. Look at MySQL site for information.

Common Filters

Common filters help to reduce the amount of data displayed in reports. This is useful when you need to focus your attention on a particular time interval or on a specific sender/recipient.

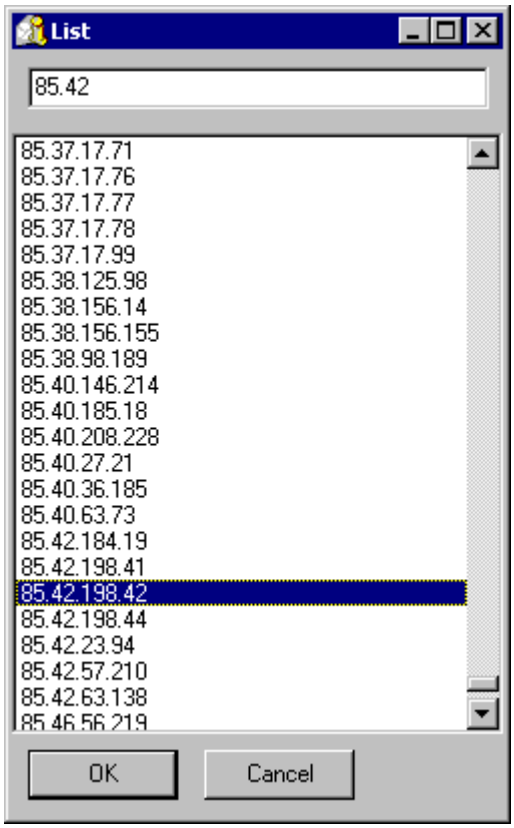
You can filter by:

- Date, specifying the interval. Only information logged between these dates will be used to generate the report.



- IP address, typing the address you are looking for activity coming from or directed to the "IP" value.

  You can use the list button  to list all the IP addresses present in the database and also search for a specific address, by typing the first few digits.

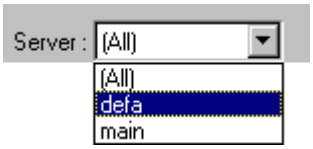


NOTE: It is also possible to use the following "wildcard" format:

80.32.*.* (or even 80.32.*)

Using only "80.32" would not work.

- Server using "Server" selector.



- Session type (client, server or both) using the "Session type" selector (look in IceWarp Mail Server manual for more information about client/server connections).