

---

IceWarp Unified Communications

# Log Analyzer – Viewer Guide

Version 10

**IceWarp<sup>®</sup>**





---

# Contents

<b>Log Analyzer - Viewer</b>	<b>3</b>
Introduction .....	3
Special thanks: .....	3
Getting Started .....	4
Log Analyzer Configuration .....	6
Import Log Files .....	7
IP Statistics .....	9
Domain Statistic .....	10
User Statistics .....	13
Global .....	14
Mail Search .....	16
Duration Statistics .....	19
Custom Search .....	20
Database Tables and Fields .....	21
ILA Tables .....	21
SMTP Table .....	21
POP3 Table .....	23
Antispam Table .....	24
Antivirus Table .....	25
MySQL Troubleshooting .....	27
Configuring MySQL external DSN .....	27
MySQL Server version 5.00 or newer .....	29

Common Filters ..... 30

**Index** **33**

---

## CHAPTER 1

# 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.

© Copyright *IceWarp Ltd.*



### In This Chapter

Getting Started.....	4
Import Log Files.....	7
IP Statistics .....	9
Domain Statistic .....	10
User Statistics.....	13
Global.....	14
Mail Search .....	16
Duration Statistics.....	19
Custom Search .....	20
Database Tables and Fields.....	21
MySQL Troubleshooting.....	27
Common Filters.....	30

---

## CHAPTER 2

---

# Getting Started

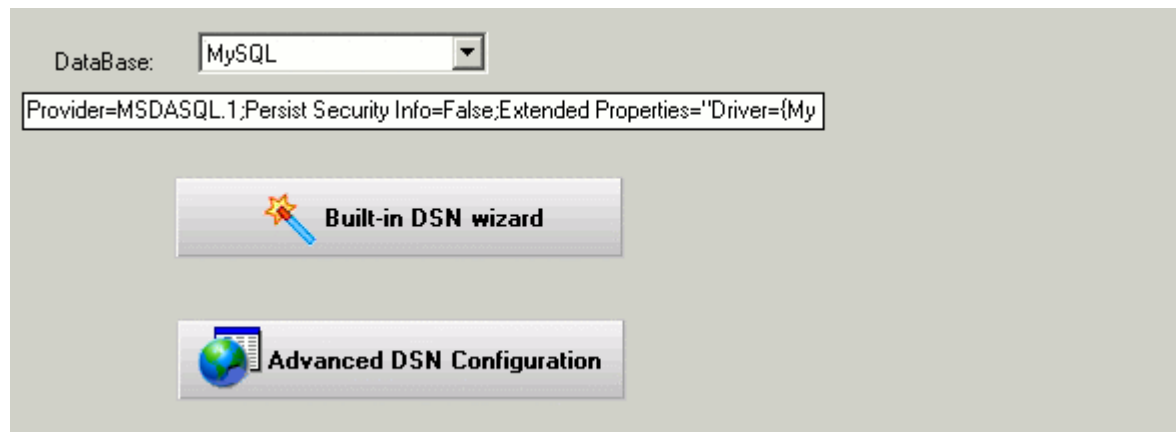
After you launched ILA, if you are in remote mode, you need to setup its initial configuration.

ILA uses an external database to operate, so you need to configure the connection to the database.

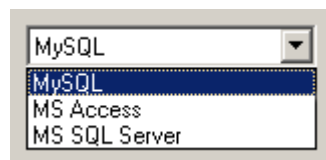
Databases supported are MySQL, MS SQL Server and MS Access so you need to choose between these databases.

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 and you must type in the database connection parameters.

Press the "Test" button to verify if the connection can be established.

Press "OK" to close and confirm the parameters typed.

Press 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 at **MySQL troubleshooting** (see "MySQL Troubleshooting" on page 27).

## **In This Chapter**

Log Analyzer Configuration .....6

## CHAPTER 3

# Log Analyzer Configuration



---

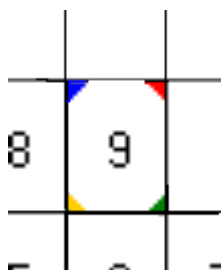
## CHAPTER 4

---

# Import Log Files

Using the Import button in ILA toolbar you can open the Import window which has 3 tabs Settings, Calendar and Manually import.

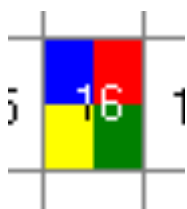
In the Calendar tab you can see a whole year calendar in which some days have small colored corner with different colors.



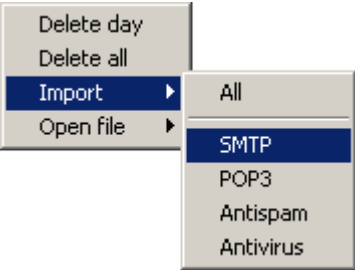
Colored corners means that there exist log files in the base log directory for the displayed day. Colors are different for different log file types:

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

After log files are imported the colors changes and occupy the entire area for that day (or square) as in the following image:



Right clicking on a day you get a pop-up menu that lets you import log files of that day. Its useful, since most administrators prefer to configure ILA importing logs of the previous day, during late night, due to performance reasons. Thus, if you want to do an analysis of something that happened after the last import, such as an email sent or received through SMTP, right button click and choose to import the SMTP log for that day, as shown below.



---

## CHAPTER 5

---

# 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:

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

Using **Common filters** (on page 30) you can focus on a part of the entire data that was logged.

## CHAPTER 6

---

## Domain Statistic



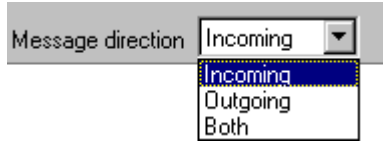
"Domain statistics" returns information about the traffic originated from or addressed to local domains.

For each domain the following information are displayed:

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

Using **Common filters** (on page 30) you can focus on a part of the entire data that was logged.

You can filter results using the message direction selector,

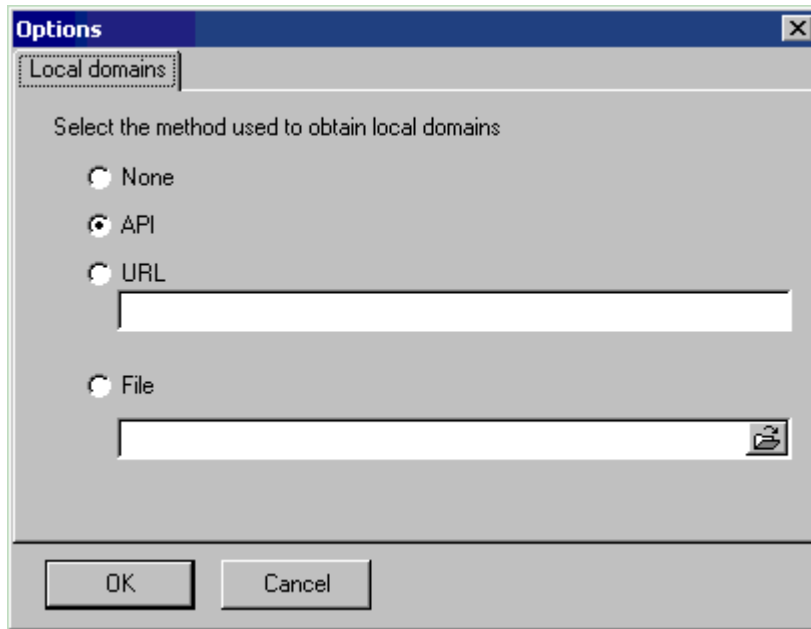


which limits the report to incoming, outgoing messages or both.

To filter a local domain only, use the "Only local domains".



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



The options are:

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

```
tool.exe export domain * > file_list.txt
```

---

## CHAPTER 7

---

# User Statistics



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

For each user the information returned is:

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

Using **Common filters** (on page 30) you can focus on a part of the entire data that was logged.

---

 CHAPTER 8
 

---

# Global



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

Messages are classified as:

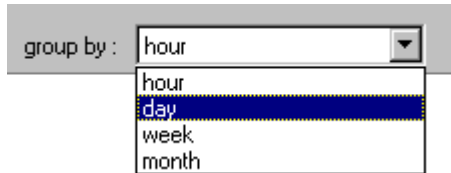
<b>OK</b>	the message was delivered correctly.
<b>DNSBL</b>	the session was refused due to a "DNS Black List" filter. The sender's IP address has been banned due to spamming or other unwanted activities.
<b>ANA</b>	the message was refused because the sender has no access permission (Access Not Allowed).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



<b>GRLS T</b>	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** (on page 30) 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.

---

## CHAPTER 9

---

# 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.

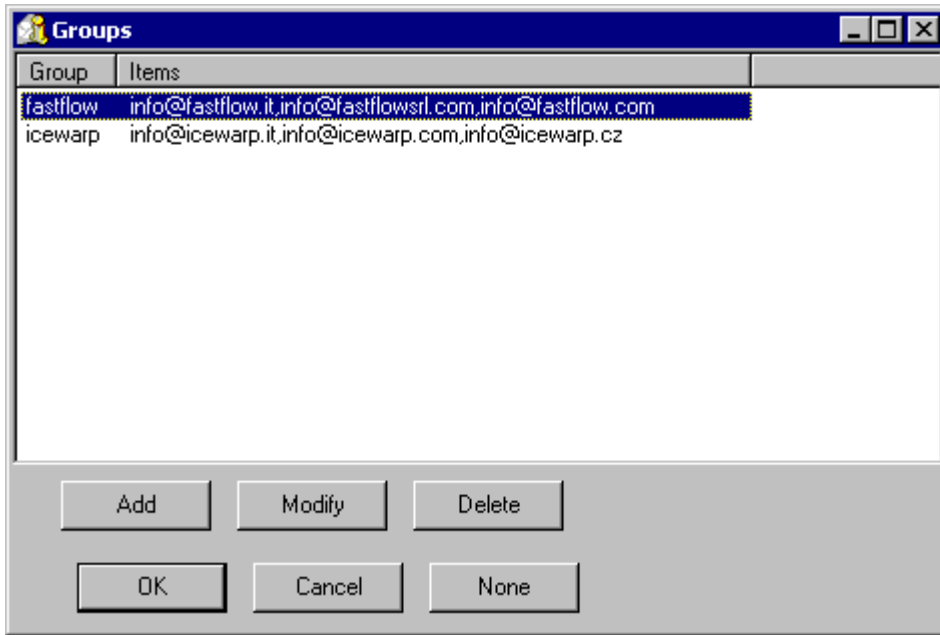
In addition to the standard **Common filters** (on page 30) you may specify a filter on:

<b>From account</b>	The alias of the "MAIL FROM" address
<b>From domain</b>	The domain of the "MAIL FROM" address
<b>To account</b>	The alias of the "RCPT TO" address
<b>To domain</b>	The domain of the "RCPT TO" address

Using **Common filters** (on page 30) you can focus on a part of the entire data that was logged.

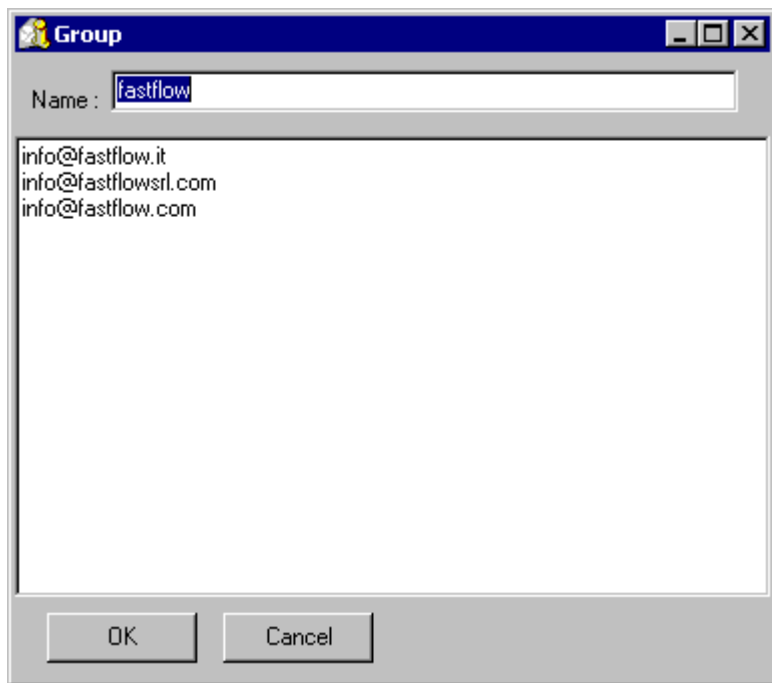
Using button list  you can list all the available from/to accounts or from/to domains and select the item you need.

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** (see "Global" on page 14) section of this guide.

## CHAPTER 10

---

## 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:

<b>MinDuration</b>	the minimum processing time for a message of this class
<b>MaxDuration</b>	the maximum processing time for a message of this class
<b>AvgDuration</b>	the average processing time for a message of this class
<b>SumDuration</b>	the total processing time for this class
<b>SumSize</b>	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** (on page 30) you can focus on a part of the entire data that was logged.

---

## CHAPTER 11

---

# 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.

---

 CHAPTER 12

---

## Database Tables and Fields

### ILA Tables

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

#### SMTP Table

<b>lg_AI recordID</b>	The record ID
<b>lg_ATRN</b>	The domain name for which the ATRN command is executed
<b>lg_ATRN_res</b>	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;
<b>lg_AUTH</b>	The result of the AUTH command execution: "N" no authentication took place; "S" user authenticated successfully; "F" authentication failed;
<b>lg_AV</b>	Antivirus response if delivered message had infected content.
<b>lg_AccessNotAllowed</b>	"Y" the message was stopped by a black list or a helo filter; "N" this condition didn't apply;
<b>lg_ClientSession</b>	"Y" the session was a client session; "N" the session was a server session;
<b>lg_DNSBL</b>	If present, this is the hostname of the DNSBL system that listed the sender's IP address.
<b>lg_Date</b>	The date of the session.
<b>lg_DeletedByFilter</b>	If present, this is the name of the filter which rejected the message.
<b>lg_DomainSenderMustExist</b>	"Y", the message was rejected because the sender domain doesn't exist.
<b>lg_Duration</b>	The duration of the session in seconds.
<b>lg_ETRN</b>	The domain name for which the ETRN command is executed.
<b>lg_Error</b>	"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; "E" 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

<b>pop_AI</b>	The record ID.
<b>pop_Server</b>	The Server ID.
<b>pop_ThreadID</b>	The Thread ID of the connection.
<b>pop_FromIP</b>	The IP address of the remote system.
<b>pop_Date</b>	The date of the session.
<b>pop_Time</b>	The time the connection started at.
<b>pop_Duration</b>	The duration of the session in seconds.
<b>pop_RETR_Count</b>	Number of messages retrieved from the server.
<b>pop_RETR_Size</b>	Total size of messages retrieved from the server.
<b>pop_DELE_Count</b>	Number of messages deleted.
<b>pop_AUTH</b>	The result of the AUTH command execution: <b>"N"</b> the command was not submitted; <b>"S"</b> authentication successful; <b>"F"</b> authentication failed.
<b>pop_Account</b>	Mailbox username.
<b>pop_Password</b>	Mailbox password.
<b>pop_Log</b>	Raw session data, compressed with ZLib algorithm.
<b>pop_LogRows</b>	Raw session data line count.
<b>pop_MsgSize</b>	The size of messages contained in the mailbox.
<b>pop_MsgCount</b>	The number of messages contained in the mailbox.
<b>pop_Error</b>	The error, in case of failure.
<b>pop_ClientSession</b>	<b>"Y"</b> a client session (remote account); <b>"N"</b> a normal POP3 session;

## Antispam Table

<b>as_AI</b>	The record ID
<b>as_Server</b>	The server ID.
<b>as_ThreadID</b>	The Thread ID of the connection.
<b>as_FromIP</b>	The IP address of the remote system.
<b>as_FromAccount</b>	Sender's alias.
<b>as_FromDomain</b>	Sender's domain.
<b>as_Date</b>	The date of the session.
<b>as_Time</b>	The time the session started at.
<b>as_MessageID</b>	The Message ID.
<b>as_Log</b>	Raw session data, compressed with ZLib algorithm.
<b>as_LogRows</b>	Raw session data line count.
<b>as_ToAccount</b>	Recipient's alias.
<b>as_ToDomain</b>	Recipient's domain.
<b>as_Score</b>	The overall spam score.
<b>as_Action</b>	The action performed by the server.
<b>as_RSBody</b>	<p>A bitmask of the following values:</p> <ul style="list-style-type: none"> <li>Parts = 0x0001</li> <li>External = 0x0002</li> <li>NoText = 0x0004</li> <li>Script = 0x0008</li> <li>Differ = 0x0010</li> <li>NoBodyNoSubject = 0x0020</li> <li>Filters = 0x0040</li> </ul>
<b>as_RSByPass</b>	<p>A bitmask of the following values:</p> <ul style="list-style-type: none"> <li>License = 0x0001</li> <li>WhiteList = 0x0002</li> <li>Trusted = 0x0004</li> <li>Outgoing = 0x0008</li> <li>Size = 0x0010</li> <li>Bypass = 0x0020</li> <li>NoUser = 0x0040</li> <li>Mode = 0x0080</li> </ul>

<b>as_RSCharset</b>	A bitmask of the following values: CharsetFilter = 0x0001 CharsetMissing = 0x0002
<b>as_RSBayes</b>	Bayesian filter score.
<b>as_RSSpamAssassin</b>	SpamAssassin score.
<b>as_RSBW</b>	"Y" black & white list has been applied; "N" no black & white list was involved;
<b>as_RSContentFilter</b>	"Y" a content filter has been applied; "N" no content filter was involved;
<b>as_RSStaticFilter</b>	"Y" a static filter has affected the action; "N" none static filter was involved;
<b>as_RSChallengeResponse</b>	"Y" challenge/response has been applied; "N" no challenge/response was involved;

## Antivirus Table

<b>av_AI</b>	The record ID.
<b>av_Server</b>	The server ID.
<b>av_ThreadID</b>	The Thread ID of the connection.
<b>av_FromIP</b>	The IP address of the remote system.
<b>av_FromAccount</b>	Sender's alias.
<b>av_FromDomain</b>	Sender's domain.
<b>av_Date</b>	The date of the session.
<b>av_Time</b>	The time the session started at.
<b>av_MessageID</b>	The Message ID.
<b>av_Log</b>	Raw session data, compressed with ZLib algorithm.
<b>av_LogRows</b>	Raw session data line count.
<b>av_ToAccount</b>	Recipient's alias.
<b>av_ToDomain</b>	Recipient's name.

<b>av_Virusname</b>	The name of the virus found.
<b>av_Filename</b>	The name of the file containing the virus.

---

# MySQL Troubleshooting

## Configuring MySQL external DSN

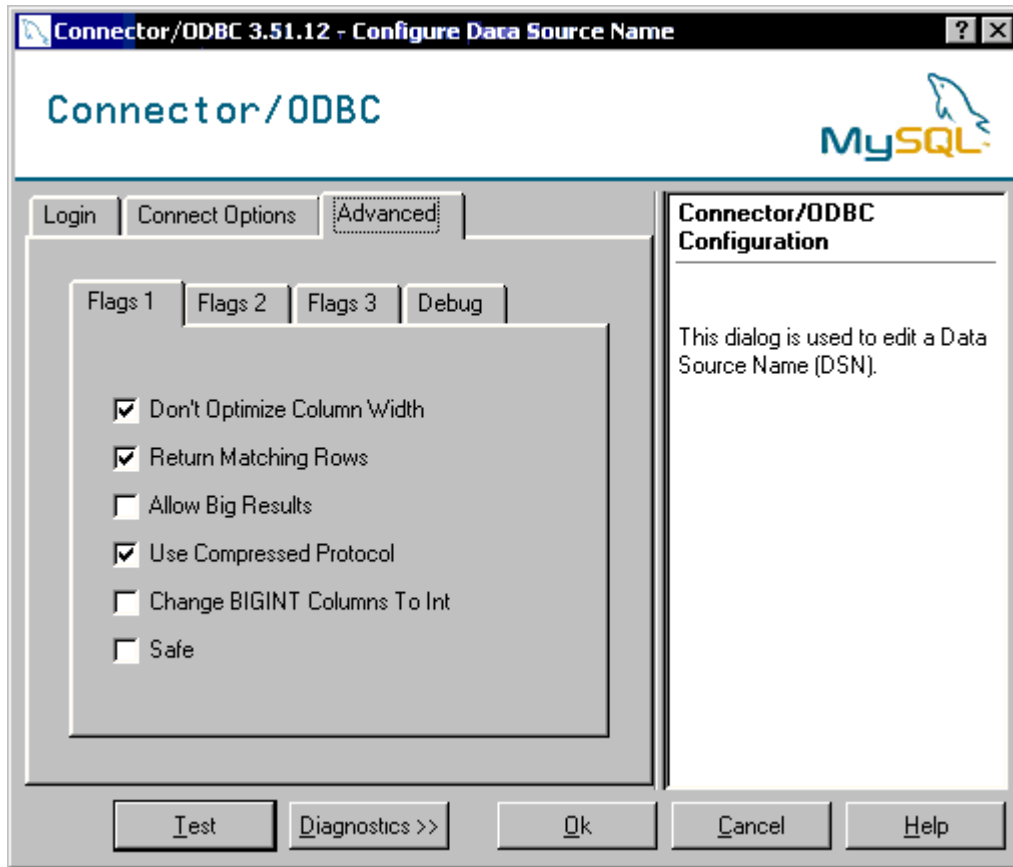
If you don't use the internal DNS configuration (it's recommended to use it) it's important to fine tune your ODBC driver's option.

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

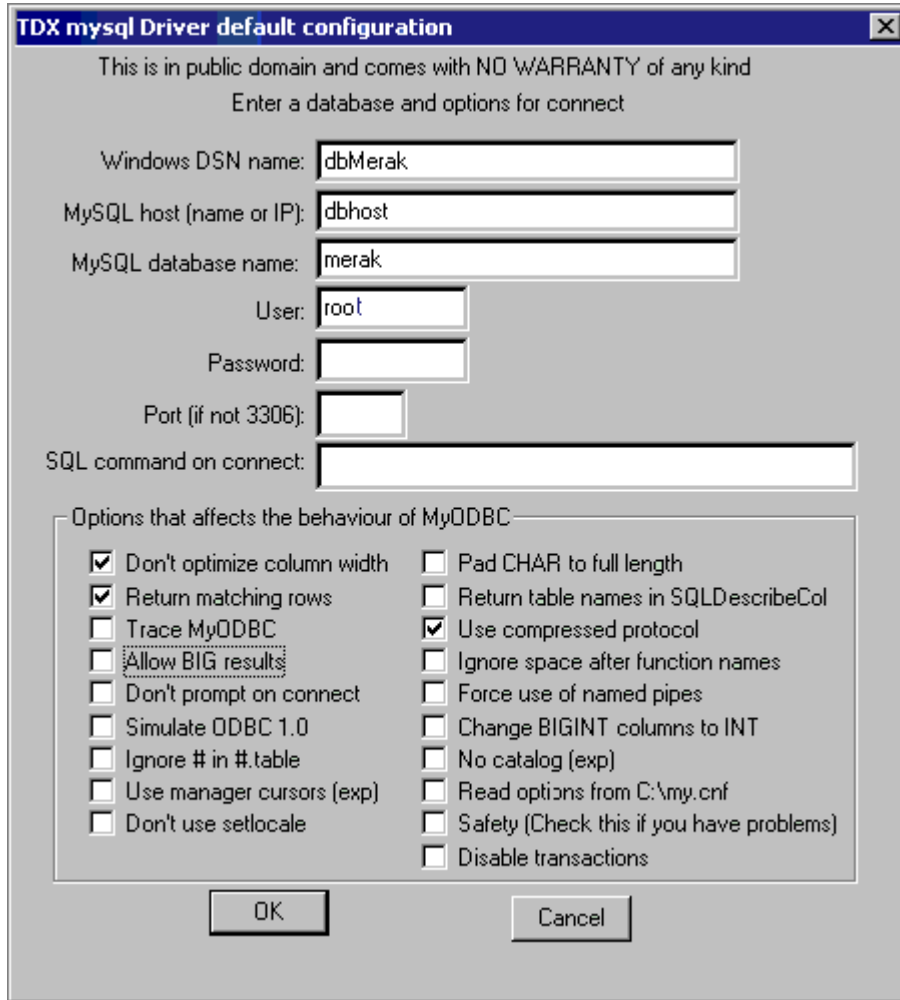
The correct configuration options for a DNS that accesses a MySQL is as follows:

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 to MySQL site for information.

## CHAPTER 14

---

## 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.


From:  18/12/2005 To:  16/01/2006

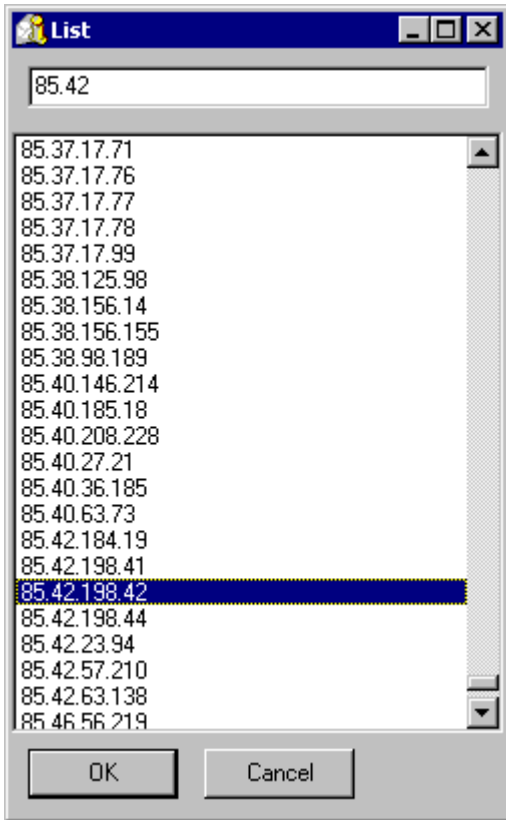
december 2005						
mon	tue	wed	thu	fri	sat	sun
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

 Today: 11/02/2006

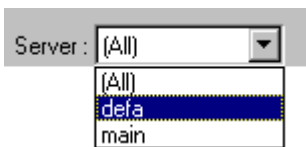


- IP address, typing the address you are looking for activity coming from or directed to the "IP" value.

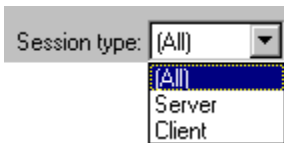
You can use the list button  to list all the IP addresses present in the database and also search for a specific address, by typing the first few digits.



- 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).





# Index

## C

Common Filters • 9, 11, 13, 15, 16, 17, 19, 30

Custom Search • 20

## D

Database Tables and Fields • 21

Domain Statistic • 10

Duration Statistics • 19

## G

Getting Started • 4

Global • 14, 18

## I

Import Log Files • 7

IP Statistics • 9

## L

Log Analyzer - Viewer • 3

Log Analyzer Configuration • 6

## M

Mail Search • 16

MySQL troubleshooting • 27

MySQL Troubleshooting • 4, 27

## U

User Statistics • 13