IceWarp Unified Communications

Log Analyzer Reference

Version 11.3

Published on 5/18/2015

Contents

Log Analyzer

The IceWarp Server Log Analyzer is a statistical and logical analysis tool for log files generated by the server engine.

Its functionality can be divided into two major areas:

- Importing the logs generated by the server as plain-text files into a database.
- Running pre-set or creating custom queries against the database to produce statistical graphs or reports for viewing or sending via email.

Each functional area is covered by its own interface with corresponding executables:

1. Built-in Log Importer (**mlaimp.exe**) configured from within Administration GUI of IceWarp Server.

   This processes raw log data from log text files and organizes this information into structured records stored in an SQL database in a form suitable for the external log Viewer application.

2. External log Viewer (ILA.exe).

   This standalone application does the analysis of the data using preset and/or custom SQL statements.

The advantage of this approach is that you can do all the configuration to collect data in the familiar Administration GUI, allowing IceWarp Server to import log files into the database automatically each night, while the external log Viewer can be run on any external machine (such as your desktop) and connect either to a local copy of the database or to a remote database (when provided with the connection details).

IceWarp Server Log Analyzer allows you to analyze your server activity quickly and efficiently over your morning cup of coffee from the convenience of your laptop.

NOTE: Currently only the SMTP, POP3, IceWarp Anti-Virus and IceWarp Anti-Spam logs are supported.

Other log types, and more detailed types of analysis will follow in the next release, along with enhanced charting, rich-text HTML statistics and other improvements to statistics reports.

NOTE: Currently (May 2015), Log Analyzer do not work in 64-bit IceWarp Server for Linux. This is a temporary state, it will be available again in the future.

Quick Start

Log Analyzer is functional immediately after installation. Its default configuration is to use a MS Access database to store data.

As soon as you open the viewer for the first time, it automatically sets up the database defined in the console (default MS Access). Make sure that the ***Database connections – Default*** option (in the viewer) is selected (bold font).

This is perfectly adequate for smaller installation with low traffic volumes. For larger installations you should consider using an industrial-strength database solution, such as MySQL or MS SQL.

NOTE: If you want to use Log Analyzer – Viewer, you still have to setup the database within the Viewer (even for MS Access), which was explained before. It is setup automatically inheriting console DB settings on the first time you run the Viewer. If you have to define the DB again in the Viewer, double-click the ***Database Connection – New*** *and setup it here.*

Do the following to start collecting data and analyze it:

Required Steps

1. In the ***Help – License...*** main menu item, verify that your license for the **Log Analyzer** module is not expired.

   (Tick the ***Display all licenses*** check box to reveal licenses for all modules.)

   If expired, contact your sales representative who will provide you with 30 day trial license.

2. Under the **System – Services – General – <service> – Logging** tab, check the ***Active*** box and on the **System – Services – General** tab select the ***Logging*** type (***Debug, Extended,*** etc.).

   NOTE: The global logging has to be enabled – use API Console – the c_system_logging_general_appendfiles variable.

3. Under **Log Analyzer – General**, check ***Active***.

   Select the logs to process.

4. Under **Log Analyzer – General**, import the data.

   Logs are imported always at 1:00 AM, so at the moment you have only the previous day logs at your disposal. You can always read SMTP log files without importing them – use the direct built-in viewer. Or import logs manually using the **Import Now** button and select the day you wish to import. It may take a while to complete this depending on the size of logs.

   NOTE: If you want to use other database than MS Access (default), you have to set this database prior to this step. See the ***Database Setting*** *section further.*

5. Under **Log Analyzer – General**, click the ***Run viewer*** button and view your data.

   IceWarp Log Analyzer application opens – when run in this way, it automatically opens the database that was configured in the GUI.

6. Click ***Apply*** to save the settings.

Optional Steps

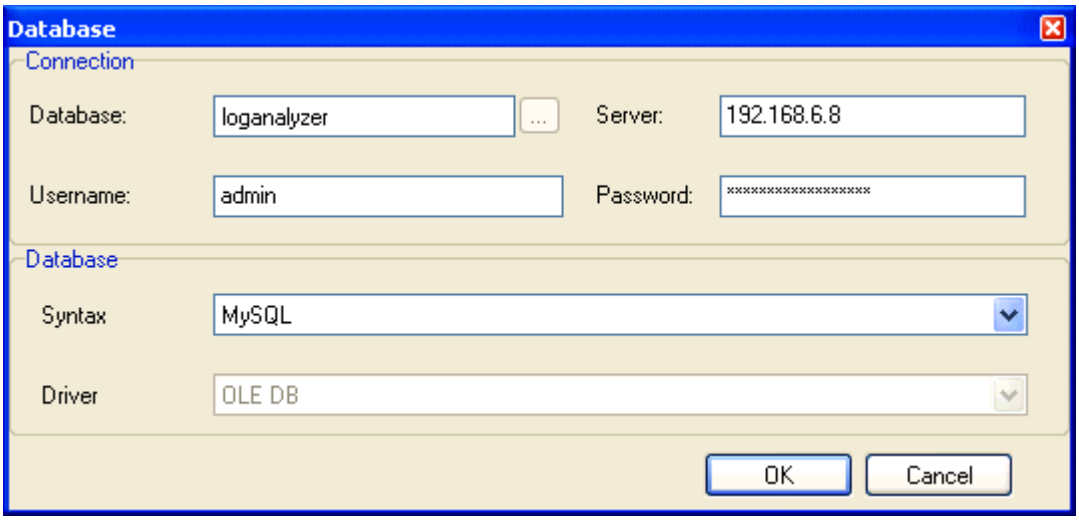
For mid-sized and larger installations, it is recommended to use MySQL or MS SQL databases instead of MS Access.

Database Setting – Windows

1. Create a database.

   Create a blank database with your database administration tools.

2. Under **Log Analyzer – General**, click ***DB Settings*** and configure the connection to the database you just created.



NOTE: This dialog is different to the standard one used elsewhere in IceWarp Server.

Field	Description
Database	Ensure you enter the correct physical or UNC path to the database file. *NOTE: The "..." button is available only when MS Access syntax is selected.*
Server	Enter either IP or a fully qualified domain name.
Username	Enter the user name used to connect the database.
Password	Enter the password used to connect the database.
Syntax	Select the database type.
Driver	Connector to the database.

3. To test the connection, click the ***Import Now*** button, then ***OK*** at the **Select Date** dialog.
4. Go to the logs directory and open the **loganalyzer\laYYYYMMDD.log** file to see the result.

   You do not have to create any DSN.

Database Setting – Linux

NOTE: Now, the Importer uses an integrated MySQL client and if not manually configured, there is no need to install the ODBC client. Skip steps 1 and 2 in this case.

1. Install ODBC driver for MySQL.

- On **RHEL 4.x**

  Install **mysql-connector-odbc** available at ***rpm.pbone.net***

  Uncomment in **/etc/odbcinst.ini** the definition for the MySQL driver

  [MySQL]

  Description = ODBC for MySQL

  //Driver = /usr/lib/libmyodbc.so **(**Aggregation functions didn't work with 2.x version)

  Driver = /usr/lib/libmyodbc3.so (DO check the value, default is wrong)

  Setup = /usr/lib/libodbcmyS.so

  FileUsage = 1

- On **RHEL 5.x**

  yum install mysql-connector-odbc

  Uncomment in **/etc/odbcinst.ini** the definition for the MySQL driver

  [MySQL]

  Description = ODBC for MySQL

  Driver = /usr/lib/libmyodbc3.so (DO check the value, default is wrong)

  Setup = /usr/lib/libodbcmyS.so

  FileUsage = 1

2. Create a DSN

   Create a DSN called **ila**, add section like one that follows to the **.odbc.ini** file in the user's home directory (***/root/.odbc.ini***)

   Example:

   [ila]

   Description= ILA

   Driver= MySQL

   Server= localhost

   Database= ila

   Port= 3306

   Socket=

   Option= 18435

   Stmt=

   User= root

3. Configure the importer

   Under the **Log Analyzer – General tab**, tick the ***Active*** box.

   Click the ***DB Settings*** button.

   In the **Database** dialog, fill in the ***Database*** field – the DSN name (created in step # 2) where Log Analyzer will write its tables.

   Fill in the ***Server*** field – the server address (IP or FQDN) where mysql is running.

   Fill in the ***Username*** and ***Password*** fields – the credentials used to connect to MySQL.

   Set the ***Syntax*** combo ***MySQL***.

   Example:

   Database = ila

   Server = 127.0.0.1

   User = ODBC

   Password = ODBC

   NOTE: Up to version 10.1 the control cannot run the importer automatically, to schedule the import process you can use a shell script like this:

   ...

#!/bin/bash
 # Launch the importer
export ICEWARPDIR=/opt/icewarp
export PATH=/usr/bin:/bin:/usr/sbin:/usr/bin:$ICEWARPDIR/loganalyzer
export LD_LIBRARY_PATH=/opt/icewarp/lib
export IWS_INSTALL_DIR=/opt/icewarp # Icewarp installation directory
export IWS_PROCESS_USER=root # User running the service
mlaimp
...

Put this into ***/etc/cron.daily***

Launch the importer and check the logs.

Advanced Configuration

1. To have a statistical overview of the logs e-mailed after the import completes:

   Under **Log Analyzer – Statistics**, click ***Active***.

   Enter the email address where you want the overview to be sent.

   Select, which log overviews you want to be included into your report.

   Click ***Apply*** to save these settings.

   NOTE: Clustered installations are supported by importing logs from multiple servers into the same database.

2. To import logs from multiple servers such as clustered installations into the same database:

   Under **Log Analyzer – General – Options**, set the ***Server ID*** feature to differentiate among servers.

   Statistics from multiple servers can be collected to a common database and analyzed through a single viewer. Each copy of the importer in use requires a server license, while the amount of Viewers in use is not limited by any client license and can be used on server, on laptop, or by all domain administrators in parallel.

   To access logs from multiple servers through the same Viewer, just use the same database for all server installations. The system also supports load-balancing installations and can identify each server in the cluster by the means of the optional ***Server ID*** tag, which needs to be set differently for each of the servers.

3. Full session log:

   The viewer allows you to view the whole session log in detail without importing the raw data into the database (see details in the **Session log without Raw Data Import** chapter). If you need to import the data, tick the *Import raw session data* check box but this results in a much bigger database size.

4. To limit the size of the database:

   By default, the system deletes statistics for log entries older than 7 days to limit size of the database. The amount of days to keep in the analysis can be set through the ***Delete data older than (days)*** option.

5. To view logs regarding the importer activity:

   The logs regarding the Importer activity are generated into the **<install_directory>/logs/loganalyser** folder with details regarding the import process. In the case the importer cannot read the server configuration, the log will be created in the **<install_directory>/loganalyser** folder.

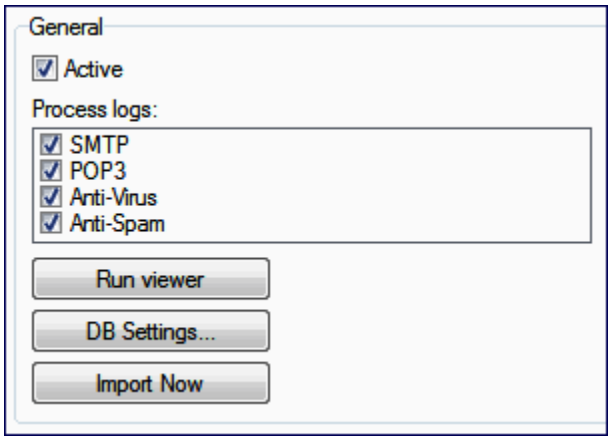
Log Importer

The Log Importer is the Log Analyzer's server-side interface.

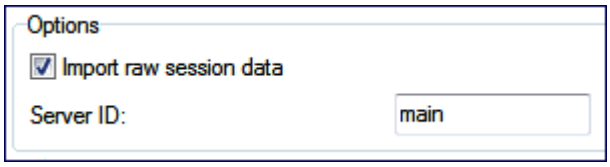
Its purpose is to import plain-text log files into database, which allow you to make standard SQL queries upon the large amounts of data accumulated.

After a one-time configuration it will work silently in the background.

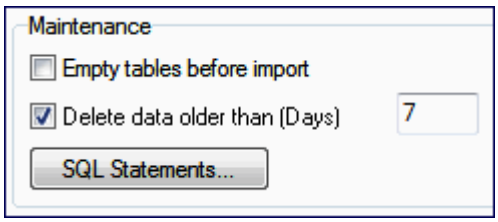
General



Field	**Description**
Active	Check this option to enable the log file import process.
Process logs	Specify which logs you want to import. *NOTE: Logging must be enabled and and selected for each log type that you want to import. See **System – Services – General – <service> – Logging** tab.*
Run Viewer	Click this button to launch the Viewer application which allows you to see your log data in a user-friendly format.
DB Settings	Clicking the button opens the standard **Database Settings** dialog allowing you to define which database Log Analyzer will be using and how to access it. Enter ***Syntax*** (type of database), server on which is established, username and password if required to access it.
Import Now	Click this button to import your log data immediately. It may take a while to complete, depending on the size of log files to process. You would not normally need to do this as the import is performed automatically every day at 01:00. The background process will only import logs generated until its launch. To view logs for the current day or a day in the past, use ***Import Now*** and select the day you wish to import from the **Select date** dialog. *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.* *Do not close the IceWarp Server console during import – the import would stop.*

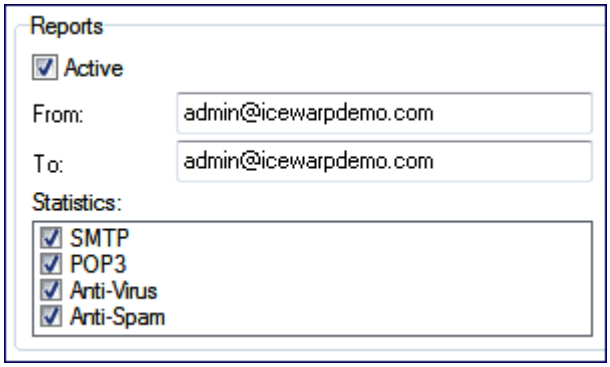


Field	Description
Import raw session data	Check this option to import raw log data into the database. This allows you to see the data as it was originally written, from within the viewer. Otherwise the importer will only transfer session data that is capable of using for the statistics. This option is deprecated and should be used carefully. See the ***Session log without Raw Data Import*** chapter for more information. *NOTE: This option will not give you any extra statistical information, just the ability to see the complete session from the log, and the possibility to use the records in custom queries.* *Checking this option will result in your database size increasing.*
Server ID	Optional way to "tag" data with a server name. This is useful where you have multiple servers and you import data to the same database as it allows you to query data for a particular server.



Field	Description
Empty tables before import	Checking this option will delete all data from the tables before importing, thus you will only have one day's worth of data at any one time (yesterday's).
Delete data older than (Days)	Check this box and enter an amount to have old data deleted before an import. This is useful to limit the size of your database and making sure the analyzer always has the last **n** days worth of data.
SQL Statements	You can specify a set of SQL statements to be executed before data is deleted. This could be used to, for example, archive a summarized view of data. Click the button to open a simple edit dialog where you can specify your SQL statements. *NOTE: The SQL is only run if you are using the **Delete data older than (Days)** option.*

Statistics



Field	Description
Active	Check this box to have Log Analyzer overview reports sent by email.
From:	Enter the email address that should be used as the ***Sender*** of the report.
To:	Enter the email address to receive the report. Multiple addresses can be specified, separated by commas.
Statistics:	Check the box against each set of statistics you wish to have included in the report.

Log Analyzer does not connects to a localhost to send report messages, the report message is put into the outgoing queue then the SMTP process will deliver it.

By default, Log Analyzer connects to 127.0.0.1.

If your SMTP is not binded to 127.0.0.1 in **System – Services**, you can bind it or change the IP using the ***HOST*** keyword in the **[STATS]** section of the **[install_dir]\config\mla.dat** file.

Example

To use 1.2.3.4 as your SMTP, you have to modify **mla.dat**:

[GENERAL]

.

.

[STATS]

HOST=1.2.3.4

Localization

The language used for reports will match the Spam/Quarantine reports configured under Anti-Spam, by means of the configuration file **– config/spam.dat** (described in ***examples/spam.dat.html***). By adding the parameter of *SpamLang=ID* where ID is the name of the folder where the language file is located, such as *SpamLang=it* for Italian.

In this example, the localization file in **/loganalyzer/lang/it/reports.xml** will be used. If however this file does not exist, the **/loganalyzer/reports.xml** file (default English localization) will be used. This file is not overwritten by upgrades (only the **/loganalyzer/lang/en/reports.xml** gets overwritten) so the administrator can customize it with their own branding or server information inside.

*NOTE: Customers upgrading from 10.x to 11.0 need to delete the original **/loganalyzer/reports.xml** file first, so that the localized file from **/loganalyzer/lang/it/reports.xml** takes effect.*

External Log Viewer Application

The external log Viewer is the Log Analyzer's user interface, where the actual log analysis takes place and the server activity over the previous day can be quickly examined.

- When run from the IceWarp Server Administration GUI, it requires no further settings to start working.
- When first run as a stand-alone application on a different computer, you will need to configure the connection to the database created by the Log Importer, using the same settings as configured on the server, but replacing the localhost with the actual IP address of the server where the DB engine is running.

Setup & Usage

The external log Viewer application can be run on any external machine (such as your desktop) and can connect to either a local database or remote one after specifying the connection details.

The application can be found in (and run from) ***<InstallDirectory>\loganalyzer***, called ***ILA.exe***. The Viewer application can be also launched by clicking the ***Run viewer*** button (**Log Analyzer – General**).

- To use local copy of the default MS Access database, no additional settings are required. (Except for database setup within **Log Analyzer – Viewer** – see further.)
- If you have chosen to use a non-default database and have configured the importer in Administration GUI accordingly, you will need to change the connection to the database by providing IP address of the server where DB is running, replacing the localhost (if inherited from the server settings), and provide the authentication details.

*NOTE: Unlike the IceWarp Server itself, Log Analyzer uses an OLE connection to the database, so you will be using yet another dialog to manage the connection – the Windows built-in utility, which allows you to select the database driver, enter the connection details and test if the connection is working. This dialog is invoked from the **Viewer** menu **– Options – Settings** tab **– Connection** – and clicking the **Advanced DSN Configuration** button.*

Help

The Viewer's help is available by pressing F1 when working with the application or selecting ***?/Help*** from the main menu.

Language

In case you prefer to switch the interface to a language other than English, you may do so in **Options – Languages**. Localizations will be added with each new version.

Database Connection

Before you can work with the Viewer, you need to connect it to the database used to store the processed statistics. It is the same database configured in the Importer section.

1. Select **Options – Connection – Settings** and select your database type.
2. Click ***Built-in DSN Wizard***.
    - If you want to use the default MS Access database, browse for the ***loganalyzer.mdb*** file in the ***<Installation Root>/loganalyzer*** folder. Click ***Test*** and then click ***OK***.

- If you have chosen MySQL database or MS SQL, you already have created a DSN and defined it in the Importer settings in the Administration console. To finish setting of the ILA Viewer, enter the same information in the Built-in DSN Wizard. Click ***Test*** and then click ***OK***.

Tips on the Viewer Usage

- In the **Options – Settings – Calendar** tab, color squares indicate what type of log is imported for each day.
- SMTP Search is very powerful. You can perform searches specifying sender, recipient and date. To speed up search times, use the check boxes next to the dates, to disable the search by date.
- Other options include traffic statistics per IP/domain/user, POP3 Search, statistics of session duration and specialized queries.

Remote Viewer Usage (while not on the server)

Please note that the Remote Administration console (available in Downloads) already includes ILA Viewer, but it is necessary to reconfigure the database connection to work from remote. This includes creating the DSN in your local machine and setting the DSN in the Administration console and in the ILA Viewer.

If you have already configured the Viewer database connection on your server, after having set the DSN locally, you can just copy this file from your server to the same folder in your local installation of the console:

<Installation Root>/config/mla.dat

You can also just copy the whole ***/loganalyzer*** folder to your local machine and run ***ila.exe*** to start the Viewer.

If you wish to run it from another location or machine just copy the whole ***loganalyzer*** directory and run ***ILA.exe***.

Configuration File

The default timeout for database connections is 300 seconds. Should the query take more than 5 minutes, it will be aborted. You can change the timeout in the ***C:\Users\<user>\AppData\Local\ila\mla_config.cfg*** configuration file by adding the following parameter:

SQL_TIMEOUT = <timeout in seconds>

It is necessary to enter this line before any other entries in the configuration file, such as DSN settings. See the example below. In this case, the timeout is set to 10 minutes.

SQL_TIMEOUT=600

DSN=Driver={MySQL ODBC 3.51 Driver};Server=localhost;Database=icewarp_ila;UID=root;PWD=paassword;OPTION=2051

Also there:

LOG_PATH = Path where the Viewer can access the mail server's log files to show the session details without importing them.

The value can be a UNC like:

LOG_PATH=\\192.168.201.105\c$\icewarp\logs\

NOTE: The user running the Viewer must have the rights to access the shared directory and the files.

Session Log without Raw Data Import

Importer and Viewer (version 0.1.87 or higher) allows you to see a session log without importing it into the database.

You have to:

- disable ***Import raw session data*** on the **Log Analyzer – General** tab
- and import a log with the new settings.

To view session details, the appropriate log file must be available to Viewer. Now, you have two ways how to do it:

1. On the server (console), open Viewer – it will find automatically the log based on the server settings.

Or:

1. In a client, you can copy the log file locally:
   - In the application base path (the directory where the **ILA.exe** executable is installed), create the **Logs** directory.
   - Copy the log files from the server (the **IceWarp/logs** folder content) to this directory with the same structure.
2. Or make available them via a user supplied path adding the LOG_PATH setting to **mla_config.cfg**:

   LOG_PATH=c:\storage\Icewarp\logs;\\storage\icewarp\logs

When the session details can not be found, Viewer will display (in **Session details)** the file name and path where looked for the file.

Support & Troubleshooting

Troubleshooting

Most common errors are caused by an incorrect configuration of the database or the database connection parameters.

Configuration varies with each different database engine and you should confirm that

- the database server is started
- the database is created
- the database contains some data
- the parameters configured in the **DB Settings..** dialog are correct.

Then use the ***Import now*** button to retry the import and look for **mlaimp.exe** process in Task Manager to see if it is running.

Then use the ***Import now*** button to retry the import, check **Status – Logs – Log Analyzer** for details on the importation process. You can also look for the **mlaimp.exe** process in **Task Manager** while the process is running

If the problem does not relate to a database or you run into issues even with the basic MS Access database, often the most effective solution is backing up the files you have customized, deleting the whole ***IceWarp\loganalyzer*** *directory, running the IceWarp Server installer of the same version you have and re-installing – this will recreate the Log Analyzer files and settings to a fresh and consistent form, without touching anything else on the server. Then you can try putting back the customized files/settings one by one to isolate the cause.*

Support & Feature Requests

We welcome any kind of feedback on the following:

- persistent issues
- reproducible bugs
- custom queries you would like included in the installation
- feature requests

Contact your support center, please.