User Manual

Documentation Version 1.3, 03/01/2011

This document contains the user manual for MegaLog Suite containing

- Presentation (TP) Version 1.3
- Pre-processor (TLPP) Version 1.3
- Main Module (TM) Version 1.3
- Database Maintenance (DBM) Version 1.3
- Tools Version 1.2
- Real-Time-Viewer (RTV) Version 2.0

Secure.IP GmbH
Leisnerweg 2
81929 München (Germany)

Author: Jürgen Schmidt
Date: 03/01/2011

Content

Overview

MegaLog Suite is an advanced Syslog server. It gives you the possibility to deal 1.000.000 events per days without losing the capability to analyse this events on different ways.

The application was developed for a LAN environment, but if you don't need the Real Time Viewer (RTV) option, it is as well suitable for WAN and/or Internet usage.

Any common and modern Internet browser is sufficient to administer and analyze the MegaLog Syslog server system.

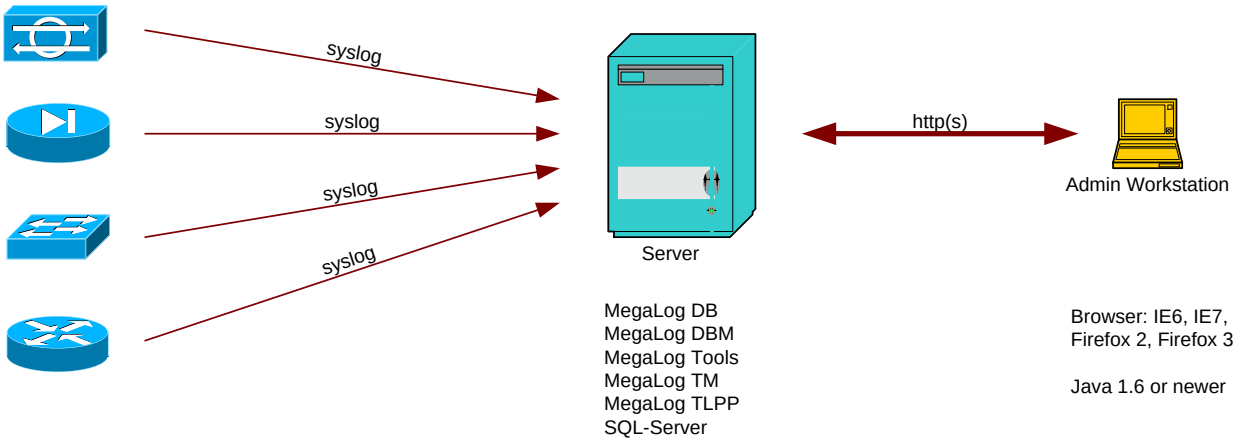
The default URL is http://localhost/MegaLog .

Special Features

- Event processing
    - analyse firewall events
    - if needed change events fields
    - hash, compress and encrypt event messages to prevent manipulation
- Event analysis
    - statistics e.g. top talker of events overview last minute / hour …
    - group analysing feature
    - host analysing feature
    - firewall analysing feature
    - drill down feature
- MegaLog 1.3 is rfc5424, rfc5426 and rfc5425 conform
- Store all events in a SQL database (primary data store)
- Automatic event export to TXT files per day/month/year (secondary data store)
- Real time viewer (RTV) for unicast and multicast sessions
- Event live time function (export to txt, compress and/or delete)

- Trigger actions (e.g. send e-mails or start batch programs)
- Programs consist of three windows services with only 3 files in a directory - no registry entries -
- MegaLog tools are stickware
- Analysing and configuration runs pure in HTML (Internet Explorer, Firefox, Chrome …)
- No special browser plug in needed (execpt Java "jre-6-windows-i586" for RTV and Silverlight - will replace all Java applet soon)
- All MegaLog services needs no MS Windows Server OS, minimum requirement is Windows XP SP3.

The best practice MegaLog installation is to install TLPP, TM, DBM and TP on the same server, but there are plenty of other combinations possible. Please have a look to "MegaLog Installation Overview.pdf"



A central Syslog server will not spare the logging systems of a server. It is common practice to use the central system to detect problems or anomalies. It can help as well to bring events from several system in a timeline.

We recommend a log level of "Warnings" for the central Syslog server instance.

Single problem are fixed by using local Syslog or Event-Log tables in combination with the central stored Syslog. Locally it is easy to enable a log level up to "Debug" and keeps the heavy Syslog traffic on the system only.

MegaLog Concept

The complete MegaLog Suite consists at least of

- TLPP (Syslog Agents and Pre-processor)
- TM (Main)
- DB (Database)
- TP (Presentation)
- RTV (Real-Time-Viewer)
- DBM (Database Maintenance)

TLPP

These modules receive events from Syslog sources (e.g. Cisco ASA/PIX) and convert it to the internal format. At this point all events can be computed with the MegaLog filter scripts for e.g. dropping of unwanted events.
It is possible to install several TLPPs for different kind of events, groups, buildings and companies on several servers.

The default network communication between module TLPP and TM is:

TCP:	TLPP:>1024	to	TM:1119	config session
TCP:	TLPP:>1024	to	TM:1120	data session

TM

This module receives the events from all TLPPs, process and store it in the database. TM exists only one time in a MegaLog installation and it can coexist with one TLPPs on the same host.
TM is the communication partner for all Real Time Viewer sessions (RTV) and inspects all events to trigger actions.

Database

You can choose your between MSSQL and MySQL databases. Tests were done with Microsoft SQL Server, Express Edition, 32 Bit and 64 Bit 2005/2008 and MySQL 5.1.

Microsoft SQL Express 2005 has a database file size limit of 2 GB. You can store round about 6.000.000 events with this "*limitation*".

The newer Microsoft SQL Express 2008 R2 has a database file limit of 10 GB. You can store round about 30.000.000 events with this "*limitation*".

If you plan to store more than 30.000.000 events, you have to use licensed Microsoft SQL server or MySQL.

The SQL database needs to be reachable via network thru standard communication paths TCP/1433 (MSSQL) or TCP/3306 (MySQL).

Important: All modules (except TLPP) needs access to the database. The database connector for MSSQL is build in .Net 4.0, for MySQL please install "MySQL Connector NET 6.3.4".

TP

The presentation module runs in an IIS environment and needs a .NET environment there. TP needs access to the database. You can use standard browsers MS Internet Explorer and Firefox. TP don't provide its own security layer, please use instead the data security function within IIS.

RTV

The real time viewer java applet will start on user's request from the presentation module (TP). The applet will start in a separate window and opens a connect to module TM.

The default network communication between module RTV and TM is:

TCP:	RTV:>1024	to	TM:1121	control session
UDP:	RTV:>1024	to	TM:12346-12362	message flow

In case of a RTV multicast session, the destination IP addresses are from 225.0.100.0 to 225.0.100.15 .

The Real Time Viewer can run in a LAN environment only. The multicast mode will only work inside a LAN without router or firewall in between. This is not a limitation of the program MegaLog; per default all routers and firewalls just block/drop multicast traffic (This default firewall setting makes sense and should not be changed).

DBM

This module takes care about the nightly statistical rollover, export events from the database to txt-files and deleting old events.

The first start of the service will create the MegaLog database. In case of software updates DBM will apply the update scripts to the MegaLog database.

DBM communicates only with the SQL server.

Common

The modules TM, DB, TP and DBM need to be in one LAN environment. The best practice installation (EasyInstaller) is to install modules on one single host.

You can install several TLPPs (Syslog agents). Because of TLPP's network communication behaviour it is easy to run this module far away, e.g. in other customer's networks or branch offices.

In case TM loose the database connection or TLPP loose the TM connection the modules still receives events. In the "Rescue Mode" the modules stores events in a flat txt-file. If the communication is re-established the txt-files will be imported to the database without loosing the correct event timestamp or anything else.

The observer/administrator can be in LAN or connected thru Internet. MegaLog is tested for the browser Internet Explorer V7 - V8, Chrome V2 - V3 and Firefox V2 - V3.

For different installation suggestions please refer to "MegaLog Installation Overview.pdf" and "Installation and Configuration MegaLog.doc".

System Installation

The system installation is described in the document "Installation and Configuration MegaLog.doc"

Basic Configuration

The basic configurations are described in the following document "Installation and Configuration MegaLog.doc"

Requirements

The system requirements are described in the document "System Requirements MegaLog.pdf".

Filter Concept

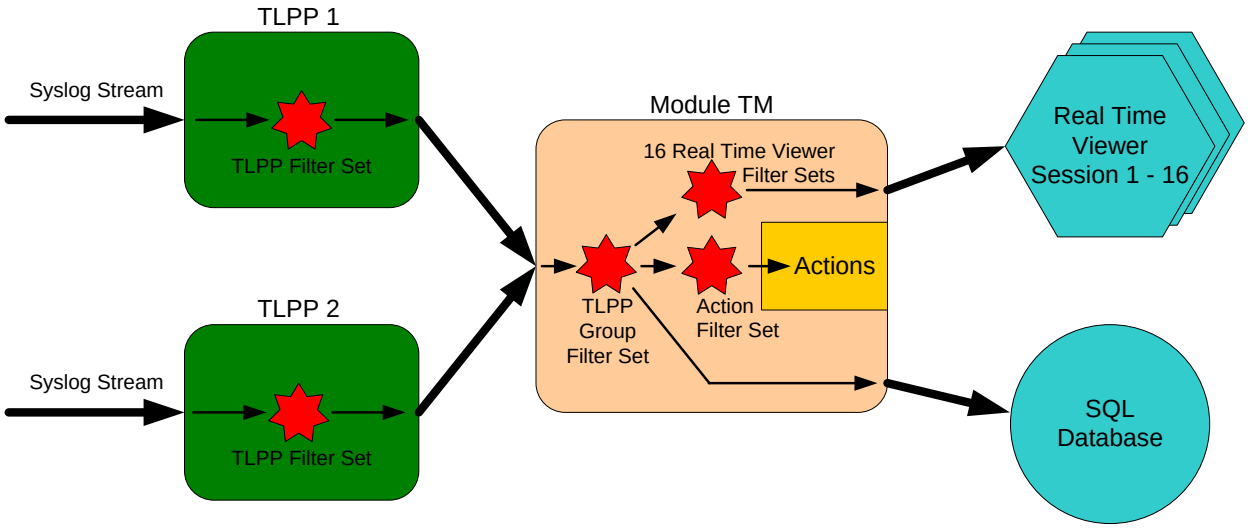
MegaLog contains a filter language optimized for speed. You can define filter scripts and apply these scripts for different kind of tasks (TLPPs, TM and RTVs).

The commands are listed in the appendix A at the end of this document. We are continuously working to improve and enhance the command set.

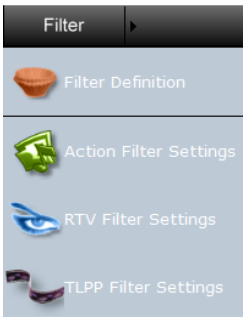
For a better performance all defined filters are loaded permanently in the module TM. Every minutes the module checks for updates. Because filter update process stops the event flow for some milliseconds, it will happen only when a real filter change was done.

Each TLPP module process up to 4 filter definitions. TLPP requests once per minute for filter definition updates and download/apply newer definitions only.

The following picture shows where the filters (see red stars) are located and in what order there are processed.



Action Filter Settings



Manage filter scripts to trigger actions in case of special events occur.

The possible actions are:

- Sending a e-mail
- Starting a program
- Showing text in the "QuickViewPanel"
- Sending a Syslog message

Example:

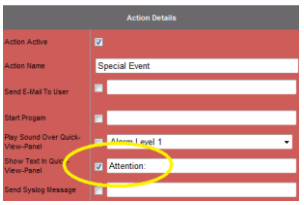
The configuration should shows messages in the "QuickViewPanel" in case of event severity is higher than "Error":

Add a new "Filter Definition" and name it e.g. "Filter Events = Error and above" with the script code:

```
if(level, <=, "3")
{
   exit(true)
}
exit(false)
```

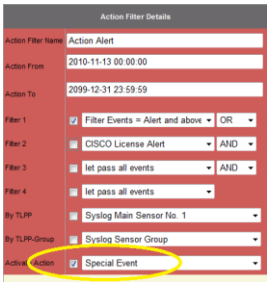
Add a new "Action" and name it e.g. "Special Events" with

- Show Text in QVP: checked
- Show Text: "Attention"



Add a new "Action Filter Settings" and name it e.g. "Action Alert" with

- Set "Filter 1" to "Filter Events >= ERROR" and activate it
- Set "Activate Action" to "Action Alert" and activate it



Real Time Viewer Filter Settings

Manage filter scripts for the Real Time Viewer sessions. In MegaLog you can define up to 16 Real Time Viewer sessions. Each session can have its own filter definition set containing up to 4 filter script definitions.

The module TM receives all messages and stores it in the database. Up to 16 copies from this Syslog stream can be send to the Real Time Viewer clients.

If no RTV client is connected neither Syslog stream copies are done nor filter scripts are wasting CPU time.

Example:

The configuration should shows events with severity higher then "Error" in a Real Time Viewer session:

Add a new "Filter Definition" name it e.g. "Filter Events > ERROR" with the script code:

```
if(level, <, "3")
{
   exit(true)
}
exit(false)
```

Change on "RTV-Filters" session id = 0, session = A to

- Rename session A to e.g. "ERROR-Stream"
- "Filter 1" to "Filter Events > ERROR"
- activate filter 1

Open RTV session A from the MegaLog menu. An additional browser window opens and the Java applet "Real Time Viewer" will show you the defined event stream.

TLPP Filter Settings

Apply up to 4 filter scripts to each TLPP:

- pre filtered and dropped events
- changes events
- analyses firewall event

Filter scripts needs to be defined in "Filter Definition" and applied to the wanted TLPP with "TLPP Filter Settings" and "TLPP Agent".

Example A:

The configuration should drop events with the severity "Debug":

Add a new "Filter Definition" name it e.g. "Filter Events = DEBUG" with the code and apply it to the TLPP:

```
if(level, =, "7")
{
   exit(false)
}
exit(true)
```

Example B:

The configuration should detect events with the text "BullShit" and declassify it to severity "Debug":

Add on "Filter Definition" name it e.g. "Filter Events = BullShit" with the code and apply it to the TLPP:

```
var(int16, a)
findpos(message, "Bullshit", "1", a)
if(a, !=, "-1")
{
   move(level, "7")
}
exit(true)
```

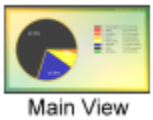
Example C:

The configuration should find all CISCO ASA or PIX events and analyse the event/message body. Additional information e.g. "Source IP Address", "Destination Port", "Protocol" and more are stored is MegaLog database field:

Add a new "Filter Definition" name it e.g. "Firewall CISCO ASA/PIX Analyser". The code in appendix B shows this example in detail. It analyse every ASA/PIX event and isolate "Message-ID, Source IP, Source Port, Destination IP, Destination Port and Protocol and store these information in the advanced MegaLog event record fields.

TP Menu

View



Main View

The main view is the start page of MegaLog. It presents several statistics in graphical form. The source of all data are the stored events and statistics in the SQL database. All graphs will update automatically once per minute. On the left side there are 5 buttons to switch between:

1. Total received event statistics for the last minute, drawn as pie chart.
2. Total received event statistics for the last hour.
3. Total received event statistics for the last day.
4. Total received event statistics for the last month
5. Total received event statistics for the last year.

If you click on these statistics picture you are forwarded to “TLPP Graphs”.

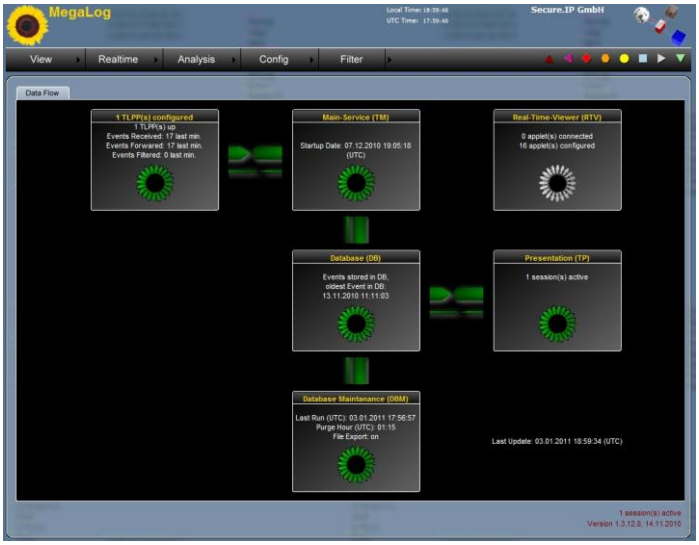
On the right side there are 3 buttons to switch between:

1. Top talker since midnight, shown in a logarithm graph.
2. Total received events of the last hour, spitted in severity and shown in a logarithm graph.
3. Total received events of the last day, spitted in severity and shown in a logarithm graph.

If you click these statistics you are forwarded to “Analyse Hosts”.

Data Flow

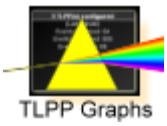
The page data flow provides detailed system information for the MegaLog services and modules.



- Status and events summaries for all TLPPs (Syslog collector and Pre Processors)
- Status and load of TM (Main Module)
- Status, stored and oldest event in the SQL database
- Status and last run of DBM (Maintenance Module)
- Status and number of active session of TP (Presentation Module)
- Status of RTV (Real Time Viewer)

Colour Code:

		Service is not running or not available	Check why services are down/not available
		Service is running normal load / normal data stream	No action
		Service is running under medium load / medium data stream	No action needed
		Service is running under high load / high data stream	Check why service is running under high load!



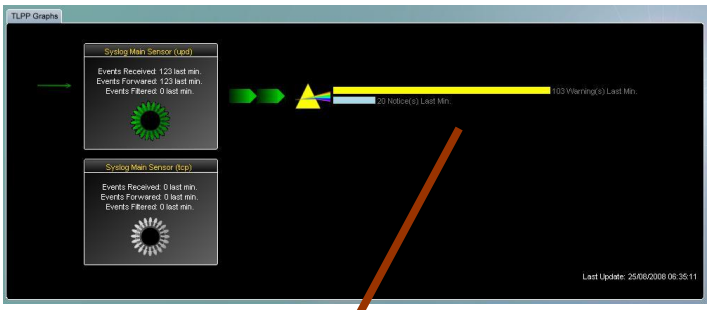
TLPP Graph

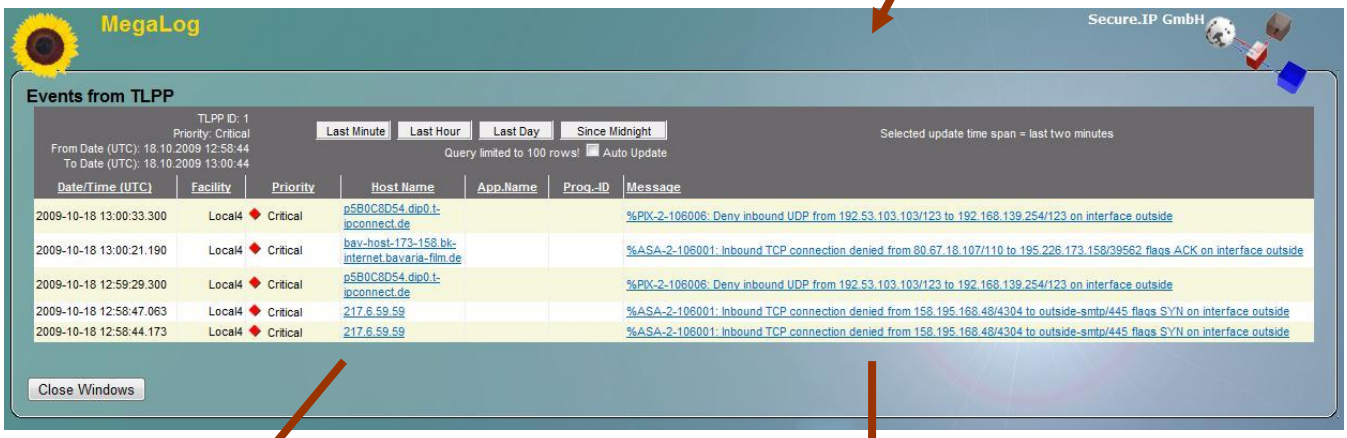
The page TLPP Graphs shows system information about the different configured TLPPs. All values are based on database information and shows the data of the past minute.

On the left side all configured TLPPs with statistical data about total event received, forwarded and dropped because of filter script are shown.

On the right side split the prism the TLPP event stream in its severity sub streams.

Click on one of the severity beams to open a popup windows.





Drill down to the host information (see Common Pop Up's)

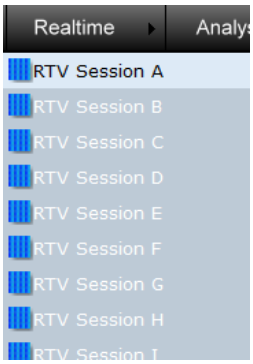
Drill down to the single event detail information (see Common Pop Up's)

Module Info

This system information module provides program related information:

- Module ID
- Module Name
- Module Version
- License
- Serial Number
- Customer ID
- Customer Name
- Company Name
- Last License Change

Realtime

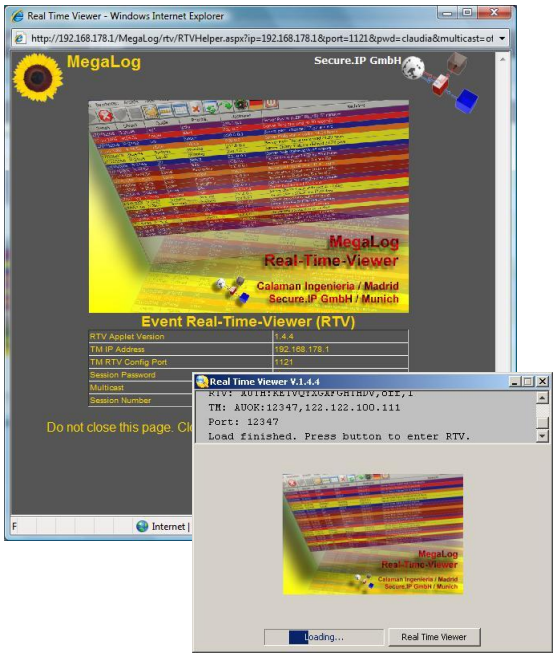


Up to 16 RTV (Real Time Viewer) session are available. The sessions with the code "A" to "N" are Unicast sessions. Only one session on administrator's workstation can use a RTV session and observe the defined real time event stream.

The session with the name "O" and "P" are multicast session. All administrators inside the LAN can join to these sessions. Because multicast network packets are dropped on the next firewall or router by default, this option can only be used inside a LAN.

Unicast Real Time Viewing

The Real-Time-Viewer is a Java applet and needs two helper pages. With click to one of the 16 session icons on the menu the helper pages are started. The helper pages check several parameters (e.g. is session already in use) and finally starts the Java program. If the helper page is closed the Java applet will close as well.



In case the session is already started you will get the following message:

Multicast Real Time Viewing

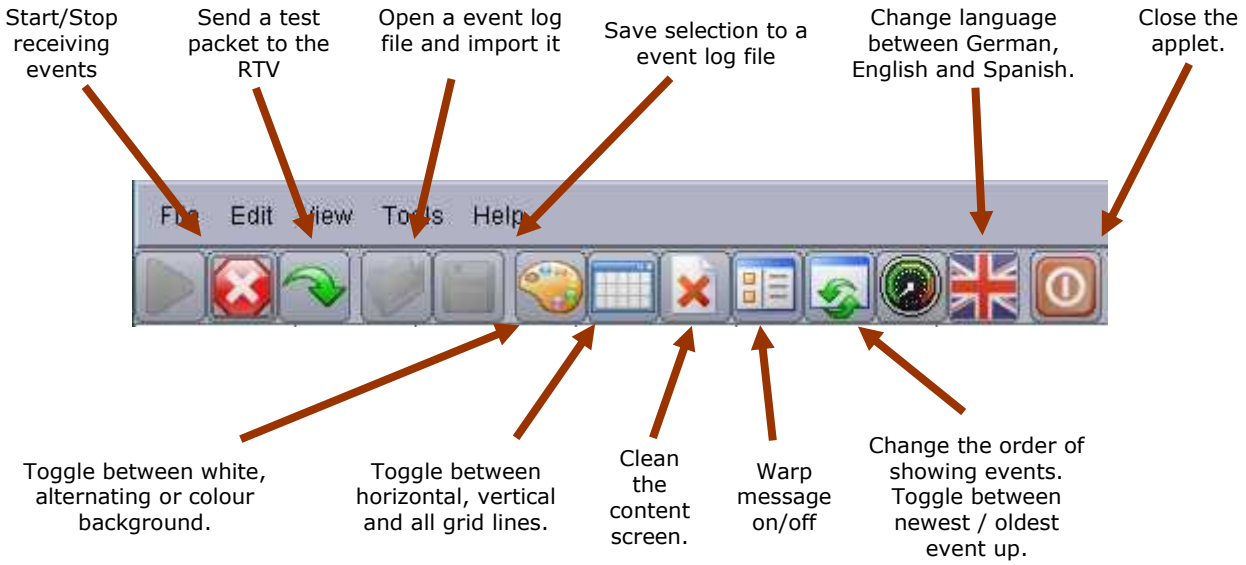
The start procedure for the multicast sessions are identically to the unicast session. Only one multicast session on the administrator's workstation is allowed. If a multicast session is already initiated by one administrator, the second administrator will join the same session.

RTV Program

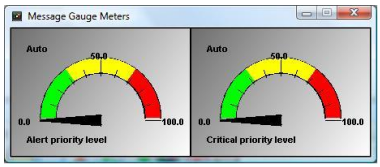
The RTV shows the incoming event in real time (the delay between Syslog agent - TLPP and RTV is less the 500 ms). Before you can use a real time viewer session you should configure a related filter. You can apply up to 4 filters per RTV session. All 16 sessions are predefined with a basic set of filter scripts. Please see "Filter" / "RTV Filter Settings" for the current configuration.

If you want to copy/paste lines or cells first stop receiving events, then select event rows and copy it to the clipboard (Edit / Copy Selected Cells). The same procedure applies for save messages to file and load a file to view.

RTV Menu



RTV Gauge



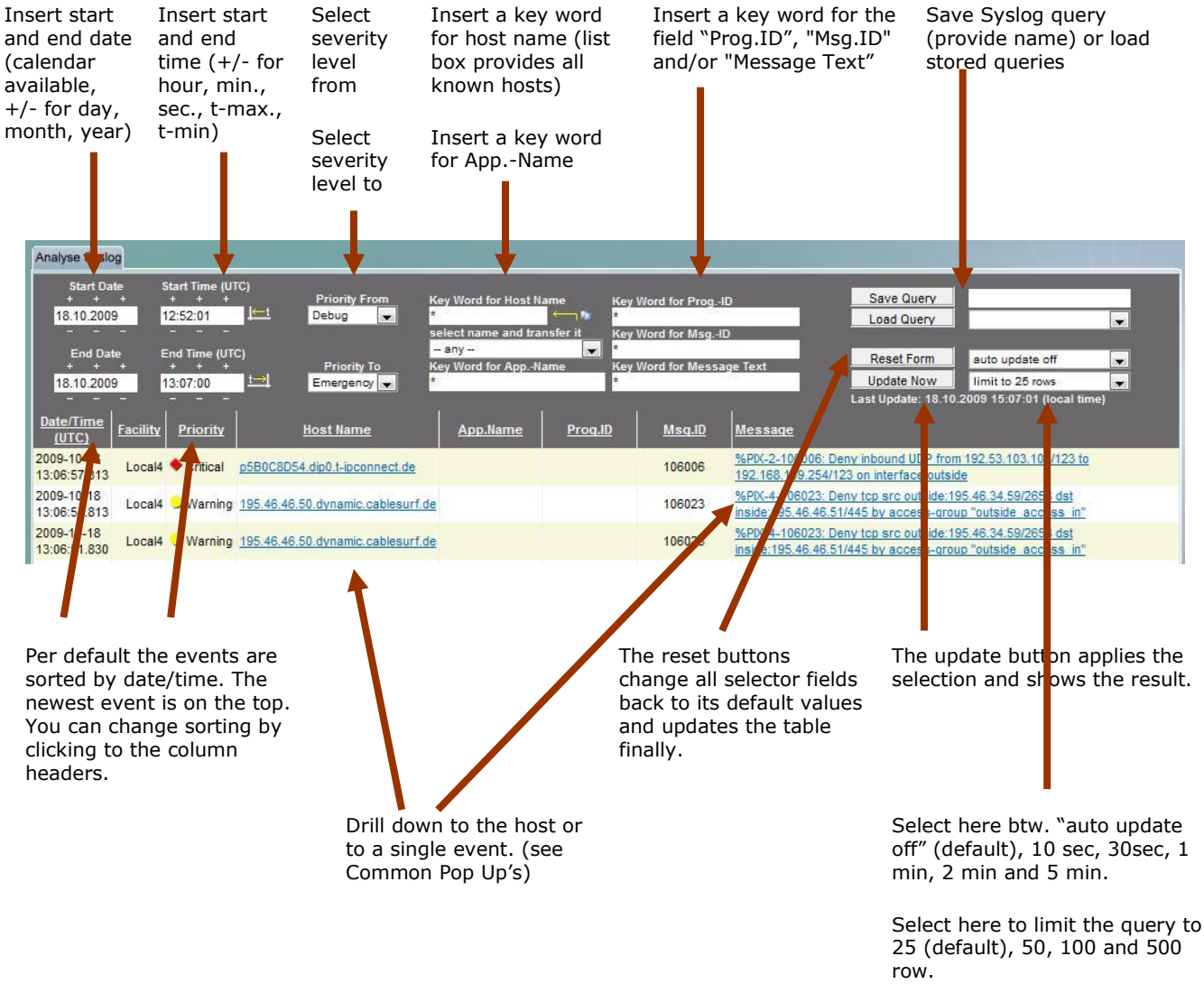
To visualize the event severity flow you can activate the gauge meters. Click on "Tools" / "Gauge Option" to configure the setting for each gauge. Disable or enable the gauges per priority here.

Analyse

Syslog

This page is the basic Syslog analysing tool of MegaLog. The focus of this analyzing tool is the time line.

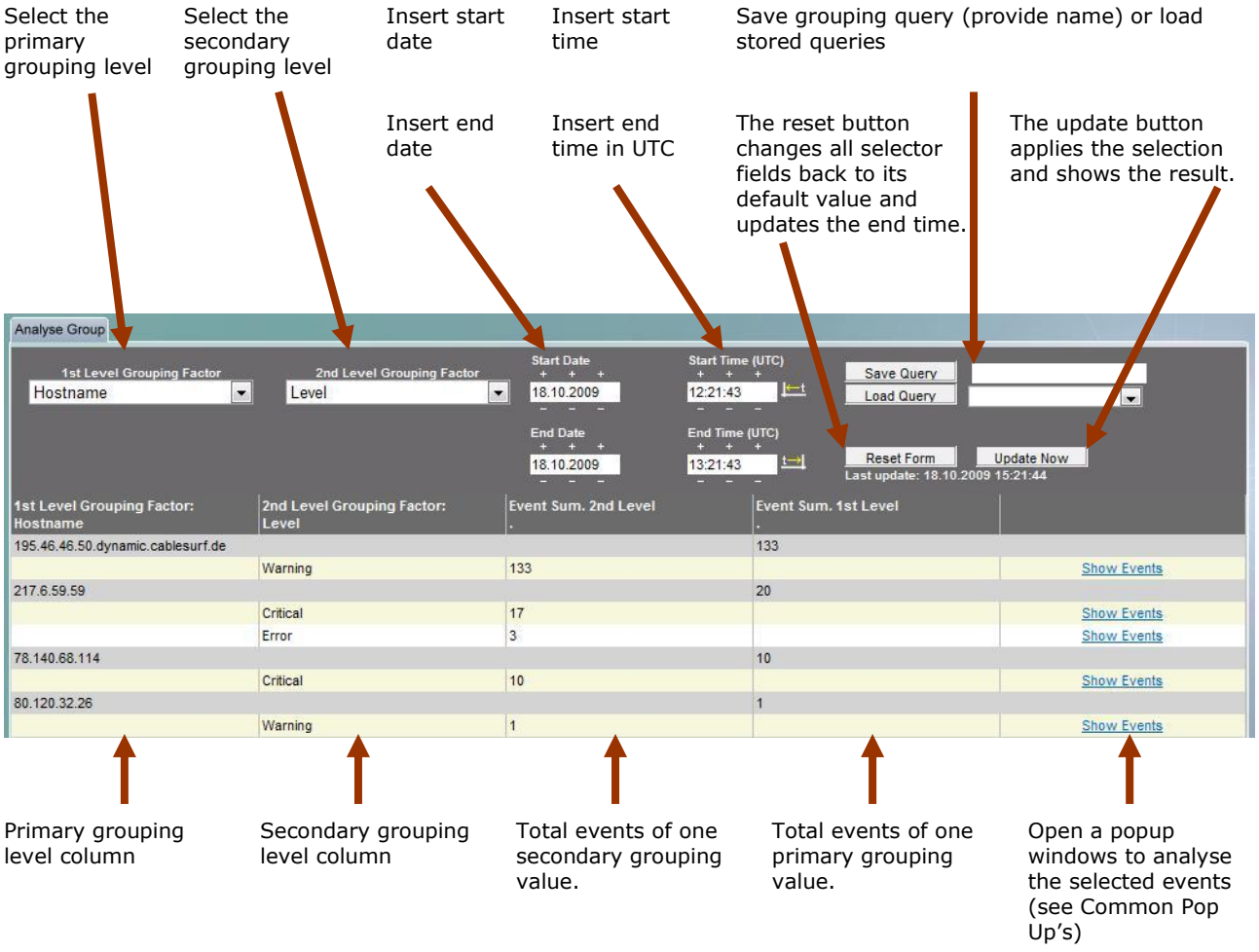
In the selector fields (Host, App.-Name, Prog.-ID, Msg.-ID and Message Text) you can use "*" and "?" as placeholder. (E.g. search string *vpn*user1* looks for strings containing "vpn" and "user1" on not defined positions!)



Grouping

This page is a enhanced Syslog analysing tools. The focus of this analyzing tool is the two level grouping function. The grouping function is available for the following event fields:

- Hostname
- Facility
- Level
- Application Name
- Program ID
- Message ID
- User
- TLPP No.
- FW Event
- FW Source IP
- FW Source Port
- FW Destination IP
- FW Destination Port



Hosts

This page is a enhanced Syslog analysing tools. The focus of this analyzing tool is the sending host.

In the selector fields you can use "*" and "?" as placeholder.

Insert a key word for host name (list box provides all known hosts)

Insert start and end date (calendar available, +/- for day, month, year)

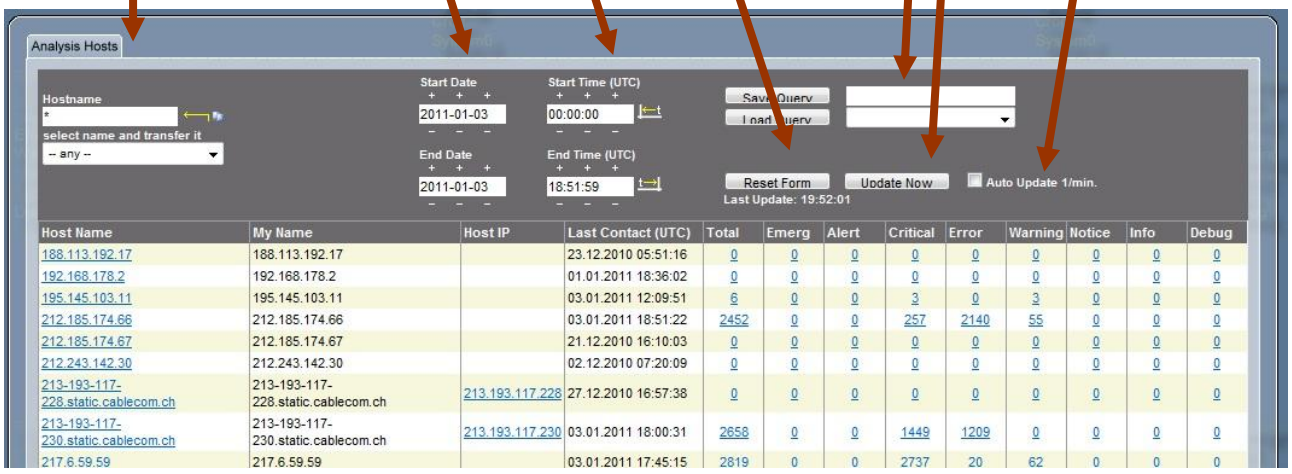
Insert start and end time (+/- for hour, min., sec., t-max., t-min)

Save hosts query (provide name) or load stored queries

The reset button changes all selector fields back to its default value and updates the end time

The update button applies the selection and shows the result.

If you check "Auto Update" the chosen selection will updated automatically every minute.



Drill down to the host details.

Opens pop up window to analyse the selected events with further drill down functions

Drill down to the host information (see Common Pop Up's)

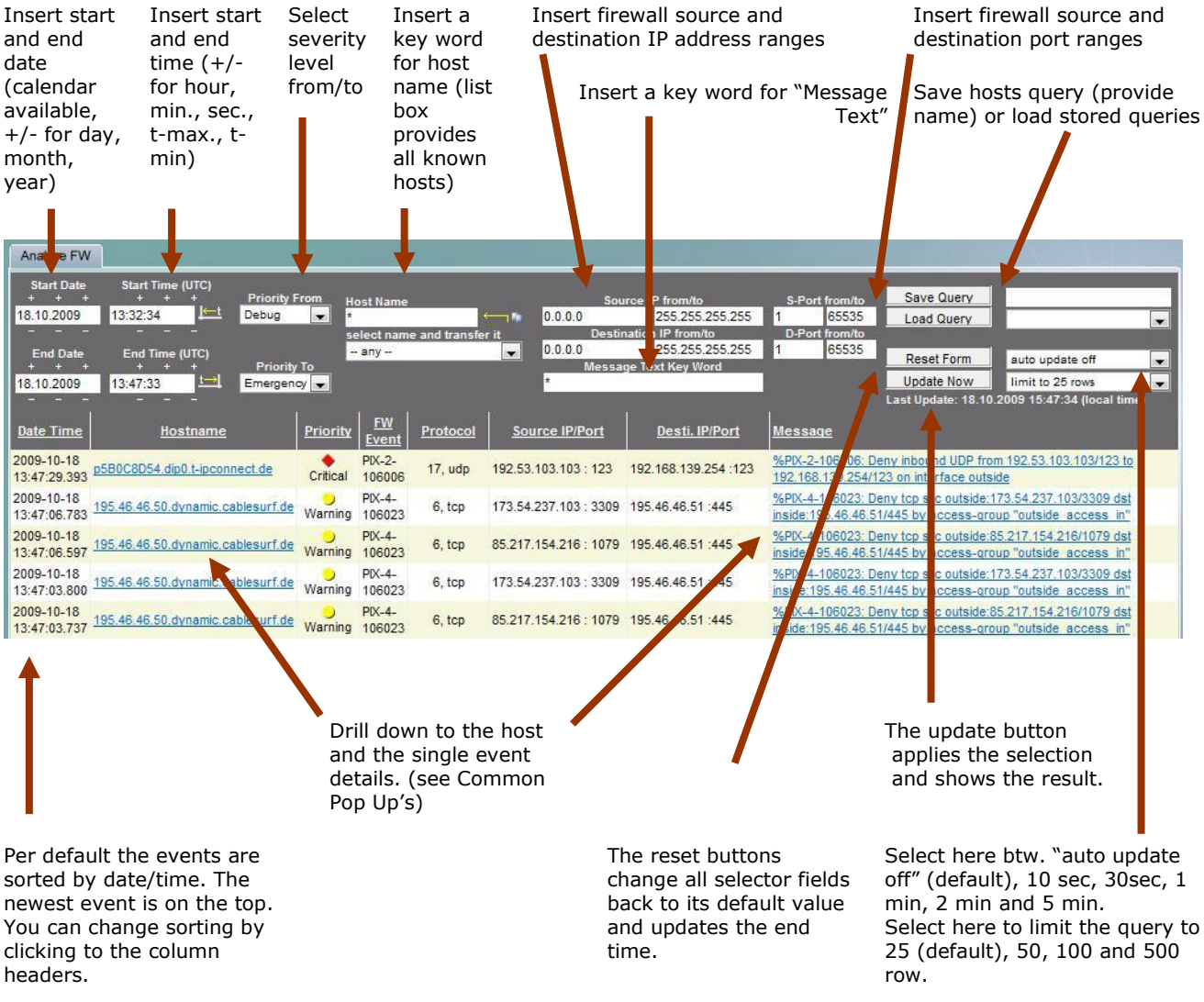
Drill down to the single event detail information (see Common Pop Up's)

Firewall

This page is a enhanced Syslog analysing tools. The focus of this analyzing tool are firewall events. To analyze events from firewalls or IDSs the packets needs to be prepared at TLPP or TM level by one or more filter processes.

The prerequisite to see firewall/IDS events is the correct usage of the field "fwsourceip". It will work best if the fields "fwsourceport", "fwdestinationip", "fwdestinationport" and "fwport" are filled by a filter process. An example is documented in annex Filter Example.

In the selector field "Message Text" you can use "*" and "?" as placeholder. (E.g. search string *vpn*user1* looks for strings containing "vpn" and "user1" on not defined positions!)

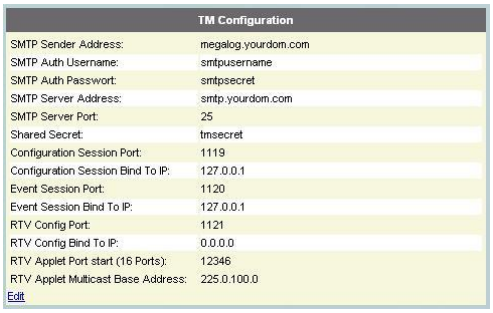


Config

TM Config

This page is for changing the TM service configuration. The main service is responsible to receive events from all connected TLPPs and stores the events in the database.

SMTP Sender Address	TM uses this entry as sender address for sending e-mail.
SMTP Auth Username	TM uses this user name to authenticate at relay host.
SMTP Auth Password	TM uses this password to authenticate at relay host.
SMTP Server Address	TM uses this IP address/host name to deliver e-mails.
SMTP Server Port	TM uses this port to deliver e-mails.
Shared Secret	The communication in the config session between TLPP and TM is protected by this password. ***Important:*** This is one start up parameter for a TLPP service.
Configuration Session Port	TM will listen on this port for a configuration session from TLPPs. ***Important:*** This is one start up parameter for a TLPP service.
Configuration Session Bind to IP	TM binds the configuration session to this local IP address. (Local means in this context where the service TM is running.) There are three cases possible: - "0.0.0.0" binds to all local interfaces - "127.0.0.1" bind only to local host only, this means that only service on the same host can access TM - "real-IP" binds it to the dedicated interface with the mentioned IP address. ***Important:*** You need to know the exact valid IP address because it is a start up parameter for a TLPP service.



TM Configuration	
SMTP Sender Address:	megalog.yourdom.com
SMTP Auth Username:	smtpusername
SMTP Auth Passwort:	smtpsecret
SMTP Server Address:	smtp.yourdom.com
SMTP Server Port:	25
Shared Secret:	tmsecret
Configuration Session Port:	1119
Configuration Session Bind To IP:	127.0.0.1
Event Session Port:	1120
Event Session Bind To IP:	127.0.0.1
RTV Config Port:	1121
RTV Config Bind To IP:	0.0.0.0
RTV Applet Port start (16 Ports):	12346
RTV Applet Multicast Base Address:	225.0.100.0

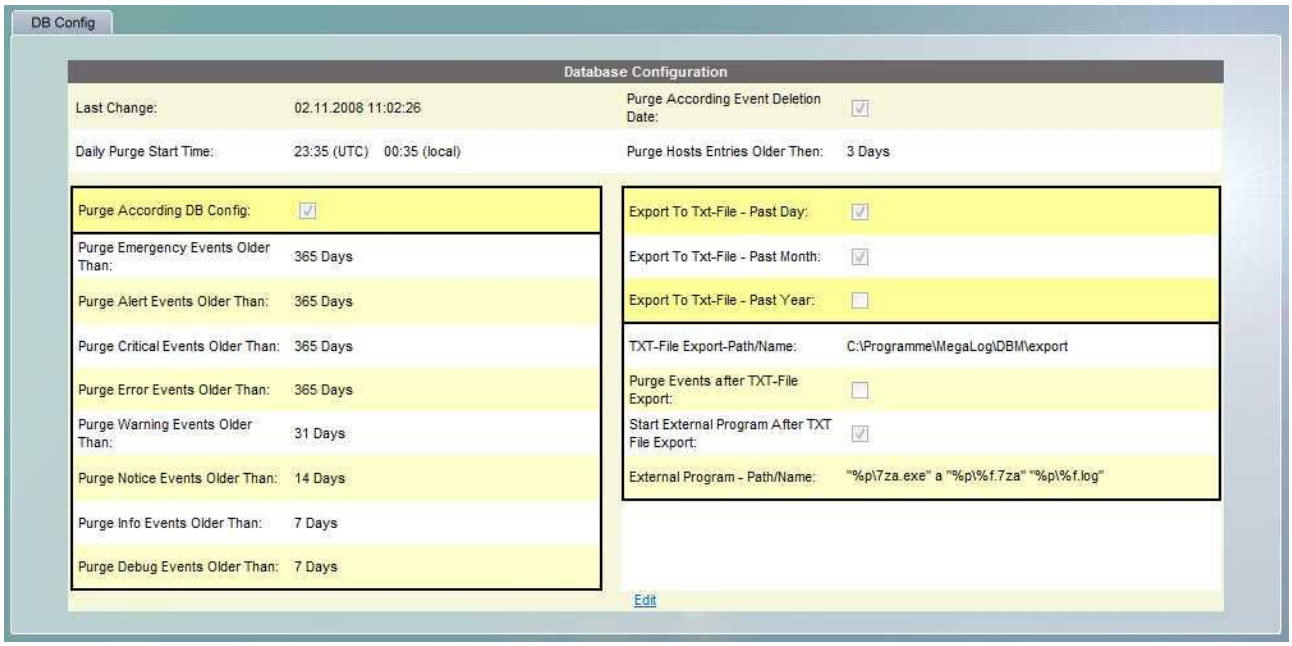
Edit

Event Session Port	TM will listen on this port for a data session from TLPPs.
Event Session Bind to IP	TM binds the data session to this local IP address. (Local means in this context where the service TM is running.) There are three cases possible. (same as "Configuration Session Bind to IP")
RTV Config Port	TM will listen on this port for request from RTV applets.
RTV Config Bind to IP	TM binds the RTV configuration session to this local IP address. (Local means in this context where the service TM is running.) There are three cases possible. (same as "Configuration Session Bind to IP")
RTV Applet Port start	TM provides this port number (plus session ID) to RTV applet during the establishment of a session. The applet should listen to this port for the UPD data stream.
RTV Applet Multicast Base Address	If the RTV Applet is requesting a multicast session, then TM provides this multicast IP address (plus session ID) to the RTV client. Default multicast IP for MegaLog RTV applets is 225.0.100.0, valid multicast IP addresses are 225.0.0.0 - 238.0.0.0.

The config file "TMService.exe.config" contains only one parameter – the connection string.
Information about the start up parameters is documented in "Installation and Configuration MegaLog.pdf".

DB Config

This page is for changing the DBM service configuration. The database maintenance service is responsible to delete outdated events regarding the parameters on this page, export event records to txt files in combination with starting an external program after.



Last Change	This field is read only and shows the date and time for the last configuration change.
Daily Purge Start Time (UTC)	Insert here what time (UTC) the maintenance process should start. The maintenance process contains event deletion, host deletion, event export and starting of one external program. The statistical roll over is always 00:00 local time and cannot be changed.
Purge According Event Deletion Date	Every event is tagged with a deletion date during the TLPP process. Per default this is 365 days. You can change this value in the TLPP Agent administration. If you want to delete it by this trigger check this field.
Purge Hosts Entries Older Then	Per default this is 365 days. If a host did not get in contact to one of the TLPPs (sending one event) it will be deleted from the MegaLog Database. The stored events for this hosts stays untouched.
Purge According DB Config	Check this field if you want to delete old events by its severity (settings in box below are active)
Export To TXT File – Past Day/Month/Year	Check one or more of these fields to export automatically the stored events in a flat txt file. If at least one export option is checked the settings in the box below are active. The file name convention is defined as: Export-Range + Date + Extension e.g.: day_2008-07-30.log, month_2008-02.log, year_2008.log
TXT-File Export – Path/Name	Insert here the drive and path where the export process should store the TXT file. Drive and path needs to be local resources of the server where the service DBM is running. Please don't finish with a "\" you input line.

Purge Events after TXT-File Export	Check this field if you want to delete the exported events from the database permanently.
Start External Program After TXT File Export	Check this fields if you want to start a external program after the file export (e.g. a zip program).
External Program – Path/Name	Insert here the drive, path and program name to start after the file export. - Use variable **%p** to get the file export path - Use variable %f to get the filename of the reasoned exported file (without the extensions) If your name contains spaces put the parameters and/or program-path-name in " e.g. "%p\7za.exe" a "%p\%f.7za" "%p\%f.log" You need to take care about the access rights to all needed directories! If you plan to start something complex you it could be a good advice to start only a command batch and do the stuff there. Even for debugging this is the preferred option.

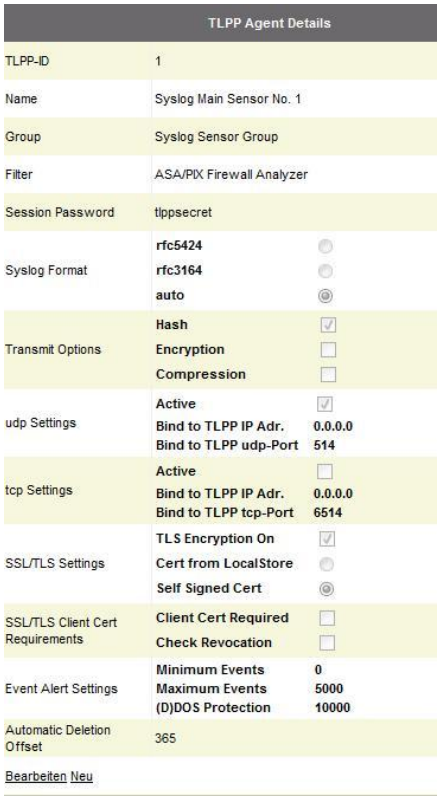
TLPP Agent

TLPP agents needs a configuration record in the database. The key value to connect the windows service TLPP with the database record is the TLPP-ID. This parameter is a parameter in the TLPP config file "TLPPService.exe.config". For more details about the config file please have a look in the document "Installation and Configuration MegaLog.pdf".

TLPP ID	This ID is unique generated by the system. This is one of the start up parameters for the TLPP service.
Name	Insert a name for this TLPP.
Group	Select one group for this TLPP.
Filter Details	Select one set of filter for this TLPP.
Session Password	Insert a session password for the authentication between TLPP and TM in the data session.
Transmit with Hash	Check this field to hash at TLPP level the values Date/Time, Facility, Severity, Host-IP and Event-Message.
Transmit with Encryption	Check this field to encrypt the traffic between TLPP module and TM.
Transmit with Compression	Check this filed to compress the traffic between TLPP module and TM.
UDP Settings	Activate/deactivate UDP listener and define were the UDP listener should listen (IP address and port).
TCP Settings	Activate/deactivate TCP listener and define were the UDP listener should listen (IP address and port).
SSL/TLS Settings	Activate/deactivate SSL for TCP listener and define certificate source.
SSL/TLS Client Cert. Requirements	Decide is ssl server require client certificate and check it against revocation list.
Event Min. Alarm	Set here the minimum event/minute baseline. If it drops below TLPP sent a notification via QVP.
Event Max. Alarm	Set here the maximum event/minute baseline. If it crosses it TLPP sent a notification via QVP.
Event (D)DOS Attack	Set here the alert event/minute baseline. If it crosses it TLPP sent a notification via QVP and close the listening port for one minute.
Automatic Deletion Offset	Every event will be tagged with a deletion date during the TLPP process. Per default this is 365 days.

		ID	TLPP Name
Delete	Select	1	Syslog Main Sensor (upd)
Delete	Select	2	Syslog Main Sensor (tcp)

"Delete" or "Select" an agent on the left side. You cannot delete the last agent!



TLPP Agent Details		
TLPP-ID	1	
Name	Syslog Main Sensor No. 1	
Group	Syslog Sensor Group	
Filter	ASA/PIX Firewall Analyzer	
Session Password	tlppsecret	
Syslog Format	rfc5424	○
	rfc3164	○
	auto	◉
Transmit Options	Hash	☑
	Encryption	☐
	Compression	☐
udp Settings	Active	☑
	Bind to TLPP IP Adr.	0.0.0.0
	Bind to TLPP udp-Port	514
tcp Settings	Active	☐
	Bind to TLPP IP Adr.	0.0.0.0
	Bind to TLPP tcp-Port	6514
SSL/TLS Settings	TLS Encryption On	☑
	Cert from LocalStore	○
	Self Signed Cert	◉
SSL/TLS Client Cert Requirements	Client Cert Required	☐
	Check Revocation	☐
Event Alert Settings	Minimum Events	0
	Maximum Events	5000
	(D)DOS Protection	10000
Automatic Deletion Offset	365	

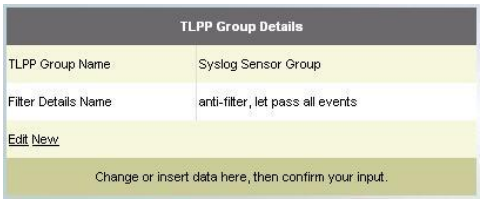
Bearbeiten Neu

"Edit" or "New" an agent on the right side.

TLPP Group

Every TLPP is member of one TLPP group. You can add, delete and change the group settings like applying a filter scripts here.

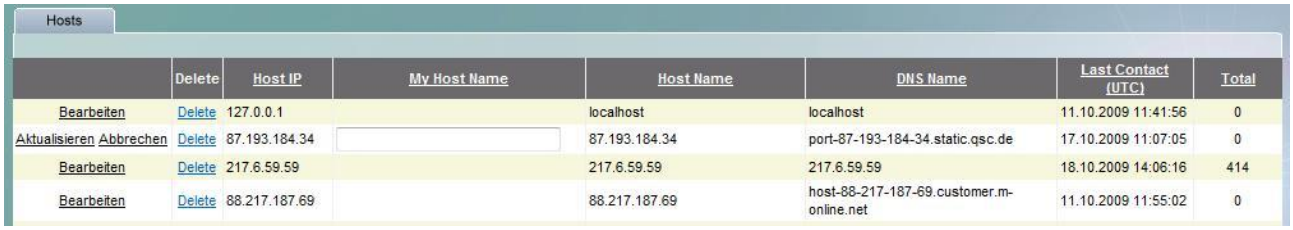
TLPP Group Name	Insert a name for this TLPP Group.
Filter Details Name	Select one set of filter for this TLPP Group.



Hosts

Administer here your host names for all system known hosts. The maintenance (DBM) process deletes hosts not received any event for more than 365 days (default) automatically. You can define the deletion parameter "Purge Hosts Entries Older Then" in DBConfig. Change or delete your host name here. Hosts are automatically created when a event is received by a Syslog agent (TLPP).

If you delete a host all associated *evens are not deleted*! You can still use analyzing queries containing deleted hosts.



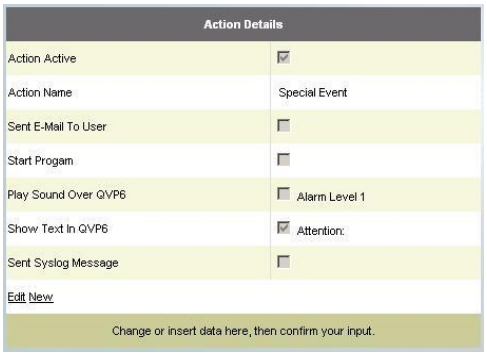
	Delete	Host IP	My Host Name	Host Name	DNS Name	Last Contact (UTC)	Total
Bearbeiten	Delete	127.0.0.1		localhost	localhost	11.10.2009 11:41:56	0
Aktualisieren Abbrechen	Delete	87.193.184.34		87.193.184.34	port-87-193-184-34.static.qsc.de	17.10.2009 11:07:05	0
Bearbeiten	Delete	217.6.59.59		217.6.59.59	217.6.59.59	18.10.2009 14:06:16	414
Bearbeiten	Delete	88.217.187.69		88.217.187.69	host-88-217-187-69.customer.m-online.net	11.10.2009 11:55:02	0

Beside the DNS name you can define your own name in the column "My Host Name".

Actions

Here you can add, change and delete actions. Actions are triggered by "Action Filter" and its definitions.

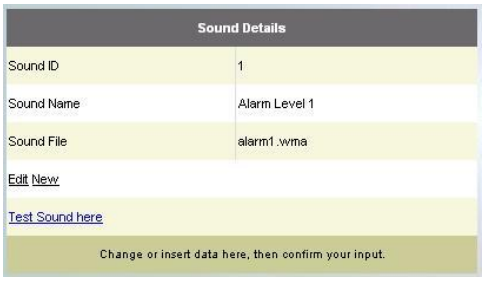
Action Active	Check this field if you want to activate this action.
Action Name	Insert a name for this action.
Send E-Mail To User	Action option 1 is to send an e-mail. Check the field to activate and insert a valid e-mail address.
Start Program	Action option 2 is to start a external program. Check the field to activate and insert a valid program drive, path and name.
Play Sound Over QVP	Action option 3 is to play a sound over the QVP (Quick View Panel). Check the field to activate and select a sound record.
Show Text in QVP	Action option 4 is to show a text in QVP. Check the field to activate and insert a short prefix like "Attention: "
Sent Syslog Massage	Action option 5 is to forward the message to a other Syslog server. Check the field to activate and insert a valid Syslog server address.



Sounds

Here you can add, change and delete sound records for using them later in actions.

Sound ID	System will provide you with a unique number. This number cannot b changed.
Sound Name	Insert a name for this sound
Sound File	Insert the file name for a sound file. The sound files needs to be stored in "…\TP\sounds". You can use the formats wav, wma and mp3.

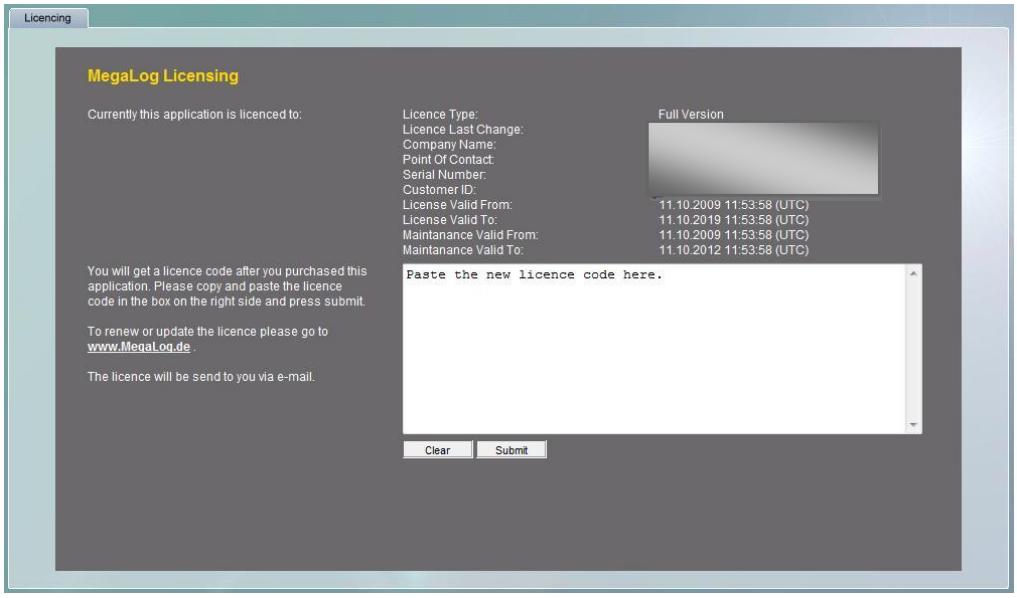


License

Add a new licenses to the MegaLog system here. MegaLog version 1.3 contains a "Free License".

After purchasing a license you have to create the license in our license centre. This is part of the MegaLog forum, a link is available at http://www.secureip.de .

Please copy the license code to the field below and press submit. After round about 30 seconds the license information will be shown there, a special status messages will be written to the error table and a message will pop up in the QVP.



Tables

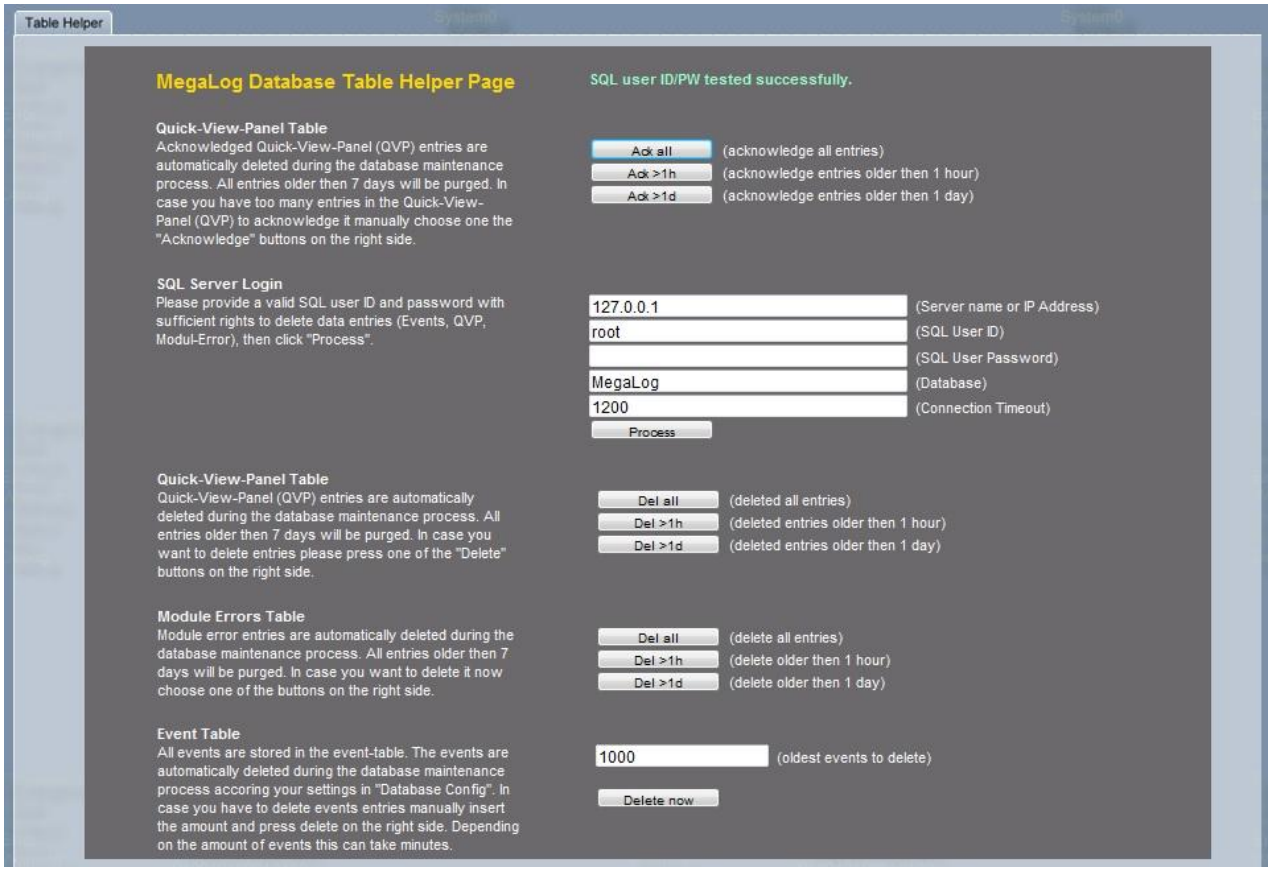
The table helper page is to administer the tables "Quick View Panel", "Error Events" and "Events". In general the tables are part for the automatic maintenance process; e.g. all event errors from MegaLog modules older than 7 days will be deleted automatically by the DBM service. Under normal conditions you do not need to take care about these tables.
In case of a service is running in the debug mode or there is a filter scripting error, it could happen, that this tables grow rapidly. In these cases you can maintain the tables here more easily then with the SQL management tools.

Without SQL Server authentication:

- Section "Quick View Panel": This sections allows to acknowledge "Quick View Panel" records.

With SQL Server authentication:

- Section "Quick View Panel": This section allows to delete "Quick View Panel" records.
- Section "Error Events": This section allows to delete "Error Event" records.
- Section "Events": This section allows to delete "Event" records.



Errors

MegaLog services send special application status messages to this error table. It depends on the messages if it is shown as well in quick-view-panel or stored in the application event message table.

ID	Timestamp (UTC)	Error Source	Severity	Error Text
2613	2010-06-02 13:06:12.640	TLPP00001	Error	Error in module EventRescue: Error in restoring event(s) from event rescue file. Disable rescue file recovery for 10 minutes! System.FormatException: Die Eingabezeichenfolge hat das falsche Format. bei System.Number.StringToNumber(String str, NumberSty
2612	2010-06-02 13:06:12.627	TLPP00001	Warning	Warning in module EventRescue: Start to restore from rescue event file to outgoing event buffer.
2610	2010-06-02 13:00:12.610	TLPP00001	Warning	Warning in module EventRescue: Start to restore from rescue event file to outgoing event buffer.
2611	2010-06-02 13:00:12.610	TLPP00001	Error	Error in module EventRescue: Error in restoring event(s) from event rescue file. Disable rescue file recovery for 10 minutes! System.FormatException: Die Eingabezeichenfolge hat das falsche Format. bei System.Number.StringToNumber(String str, NumberSty
2609	2010-06-02 12:54:12.610	TLPP00001	Error	Error in module EventRescue: Error in restoring event(s) from event rescue file. Disable rescue file recovery for 10 minutes! System.FormatException: Die Eingabezeichenfolge hat das falsche Format. bei System.Number.StringToNumber(String str, NumberSty
2608	2010-06-02 12:54:12.593	TLPP00001	Warning	Warning in module EventRescue: Start to restore from rescue event file to outgoing event buffer.
2607	2010-06-02 12:48:12.593	TLPP00001	Error	Error in module EventRescue: Error in restoring event(s) from event rescue file. Disable rescue file recovery for 10 minutes! System.FormatException: Die Eingabezeichenfolge hat das falsche Format. bei System.Number.StringToNumber(String str, NumberSty
2606	2010-06-02 12:48:12.577	TLPP00001	Warning	Warning in module EventRescue: Start to restore from rescue event file to outgoing event buffer.

Error entries older than 7 days will be deleted automatically by the DBM service.

Browser

This system page provides a browser check utility.

Browser Types:

- Firefox 3 or newer
- Internet Explorer 7 or newer
- Chrome

Features/Plug-Ins:

- JavaScript
- Java Applet
- Silverlight

Browser Information	
Browser Type :	Firefox3.0
Browser Name :	Firefox
Version :	3.0
Major Version :	3
Minor Version :	0
Platform :	WinXP
Is Beta :	False
Is Crawler :	False
Is AOL :	False
Is Win16 :	False
Is Win32 :	True
Supports Frames :	True
Supports Tables :	True
Supports Cookies :	True
Supports VB Scripts :	False
Supports JavaScript :	1.4
ActiveX Control :	False
Supports Java Applets :	True Java Version 1.6.0
Sound Check :	Sound Check

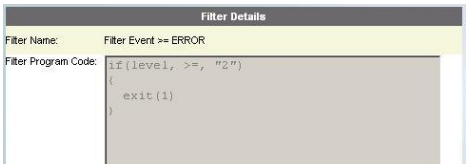
Filter

Filter Definition

MegaLog contains a filter language optimized for speed. You can define a filter scripts and apply these scripts for different kind of tasks (TLPPs, TM and RTVs).

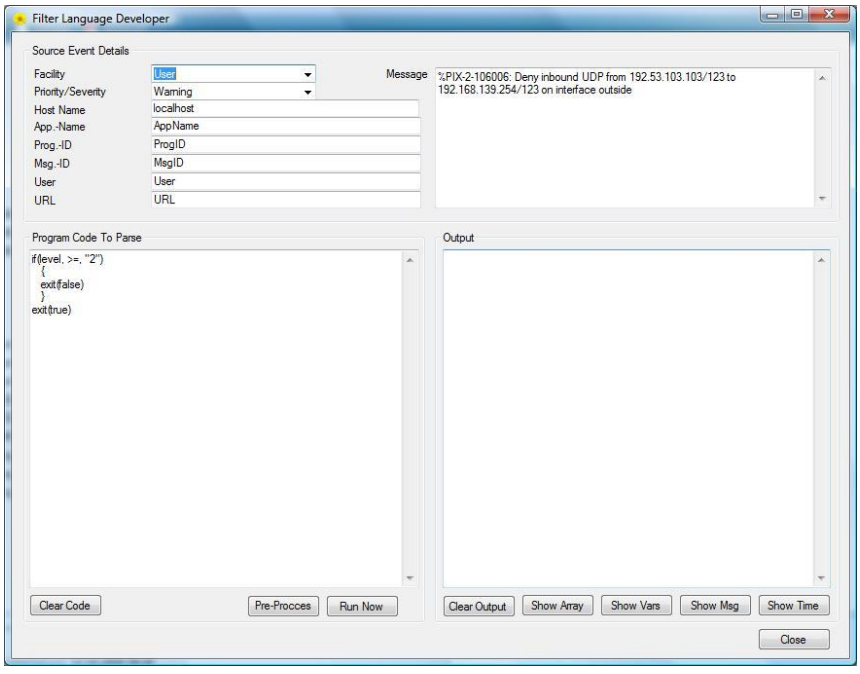
The commands are listed in the appendix A at the end of this document. We are continuously working to improve and enhance the command set.

Filter Name	Insert a name for this filter definition.
Filter Program Code	Insert here the code for this filter. Neither a syntax check can nor a test run be done here. If you have needs for this use the tool "FilterLanguage.exe".



The test program "FilterLanguage.exe" contains the same set of command but runs independently from the rest of MegaLog.

It is the perfect test program to develop filters scripts for MegaLog.



On the left side type your script and run "Pre Process". After this syntax check the program will report its result via a message box. Now you can have a look to the internal command array, for this press "Show Array".

If everything was fine, press "Run Now" and look to the results with the buttons "Show Vars", "Show Msg" and "Show Time".

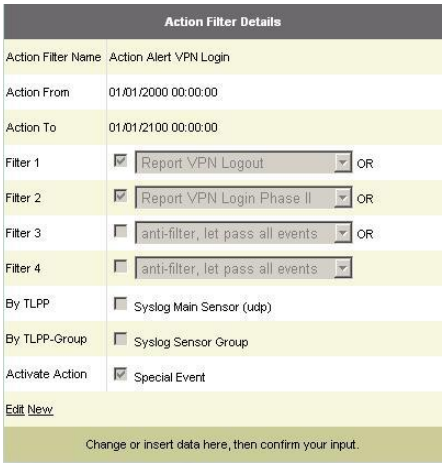
If you want check it against a real Syslog message copy/paste them to the field "Message".

After the Pre-process your code will be reformatted for better readability. During the Pre-process all remarks are removed, add the comments at the end and copy/paste the script to a "Filter Definition".

Action Filter

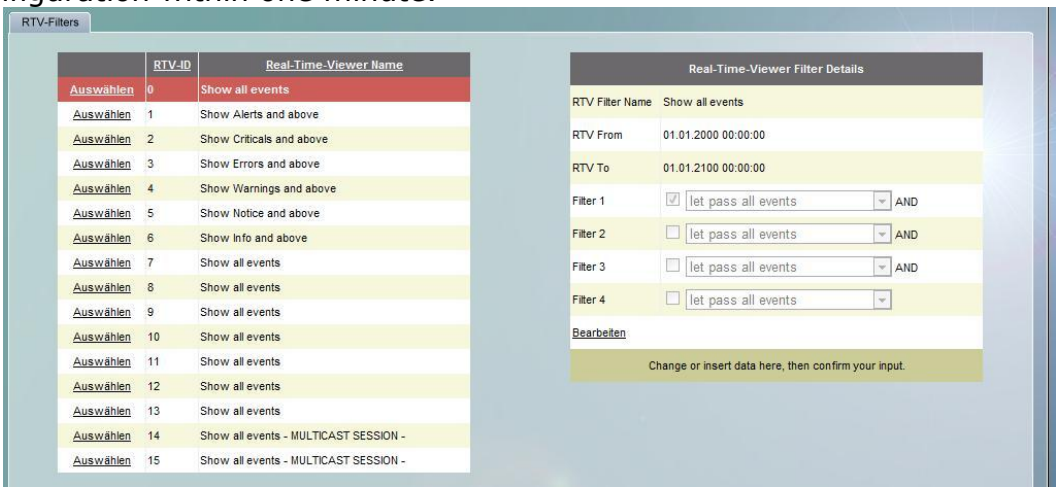
Administer here when an action should be executed in case of special events. There are several options available to filter and select on action. If you change any settings the filter inside the TM will get the new configuration within one minute.

Action Filter Name	Insert a name for this action filter set.
Action From	Insert a valid date and time from when on the filter set is active.
Action To	Insert a valid date and time until when the filter set is active.
Filter 1 .. 4	Check the field to activate this option and select one filter definition. If the complete filter chain is "True" the action will be caused.
By TLPP	Check the field to activate this option. The filter definition set will only applied to events coming thru the specified TLPP agent.
By TLPP-Group	Check the field to activate this option. The filter definition set will only applied to events coming thru the specified TLPP group.
Activate Action	Check the field to activate this option. Select a action that should be executed.



RTV Filter

Administer here the filters scripts applied to the RTV sessions (Real Time Viewer). Select one available RTV session on the left side and edit on the right side the bound filter set to this session. If you change any settings the filter inside TM will get the new configuration within one minute.



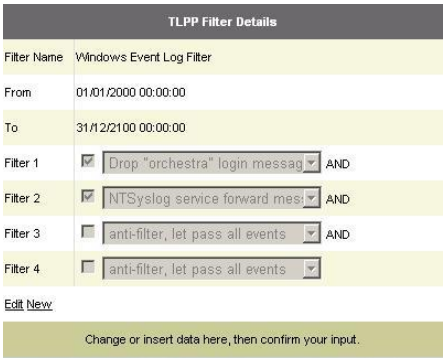
The numbers of session is limited to 16.

- Session 0 to 13 are Unicast RTV sessions,
- Session 14 and 15 are multicast RTV sessions.

TLPP Filter

Administer here the filter scripts for the TLPP agents. If you change any settings the filter on the TLPP will receive the new configuration within 1-2 minutes.

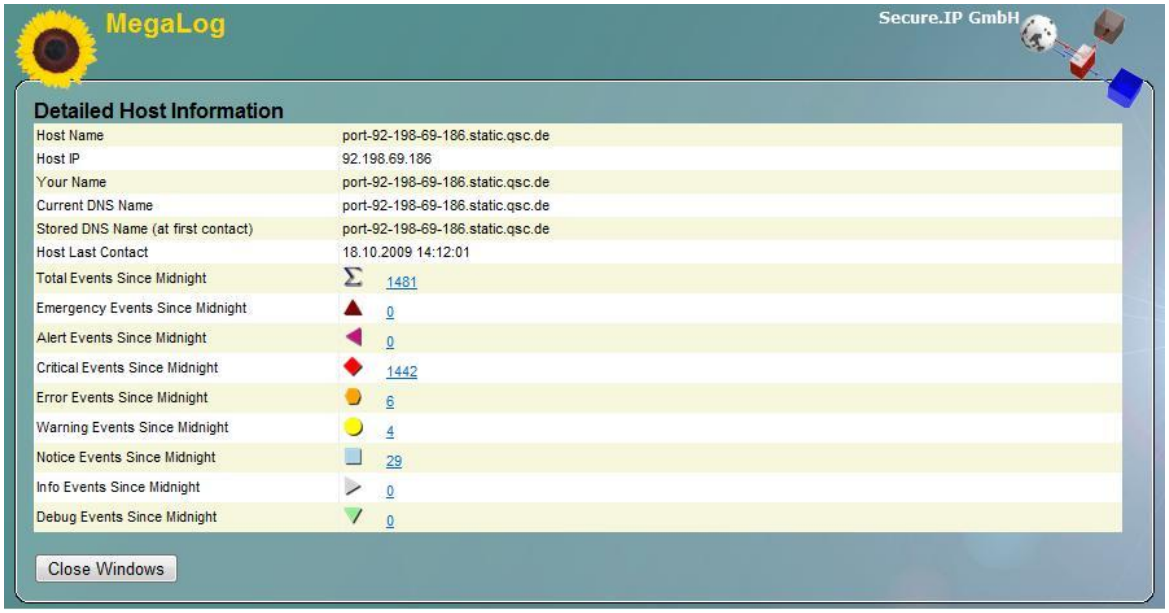
TLPP Filter Name	Insert a name for this TLPP filter set.
TLPP From	Insert a valid date and time from when on the filter set is active.
TLPP To	Insert a valid date and time until when the filter set is active.
Filter 1 .. 4	Check the field to activate this option and select one filter definition. If the complete filter chain is "True" the message will pass the TLPP.



Common PopUp's

Detailed Host Information

The most detailed information about one host you will get by the "Detailed Host Information". You can reach this pop up window thru several drill down actions.



Host IP	The unique host IP address
Host Name	In the first line you see the host name by a reverse DNS look up process during the first contact. In the second line you can see the host name by a current reverse DNS loop up.
Last Contact	It shows the date and time when the last event message was received.
Total Events Since Midnight	Here it show the total events since midnight (local time)
Other Events Since Midnight	In the following 8 line it shows the total of event separate by severity.

Detailed Event Information

The most detailed information about one event you will get by the "Detailed Event Information". You can reach this pop up window thru several drill down actions.

Event ID	Unique event ID number
Date Time	Date and time on the event
Facility	Facility of the event (e.g. 0 = kernel, 1 = user, …)
Severity	Icon and severity of the event (0 = emergency … 7 = debug)
Syslog Version	(*2) Version of Syslog packets
Host Name	Event source's host name, if possible the DNS name by reverse lookup
Application Name	(*2) Event application name
Program ID	(*2) Event program ID
Message ID	(*2) Event message ID
User	Event user name
Message	Event message
SD Time Quality	(*2) SD Time Quality
SD Origin	(*2) SD Origin
SD Meta	(*2) SD Meta
SD Other	(*2) SD Other
URL	(*1) URL of the event

TLPP No	Number of the TLPP how received this event
Firewall Event	(*1) Firewall event
Firewall Source IP	(*1) Source IP address, if possible the DNS name by reverse lookup
Firewall Source Port	(*1) Source Port, if possible name of port
Protocol	(*1) Protocol, if possible name of protocol
Firewall Desti. IP	(*1) Destination IP address, if possible the DNS name by reverse lookup
Firewall Desti. Port	(*1) Destination Port, if possible name of port
Message Hash	Messages are hashed at TLPP level, **green** = OK, **red** = tampered
Manipulated Fields	During one or more filter processes fields can be modified. Here you will see a list of all modified fields.

(*1) You will get this information only with an activated filter e.g. “PIX/ASA Analyser Filter”.

(*2) Only available in syslog version "1" regarding rfc5424, rfc5426 and rfc5425.

Playing Sound

Every time when a sound needs to be played a little pop up windows will appear. The pop up window will close automatically after some seconds.

QVP (Quick View Panel)

The QVP will be shown for special events (e.g. adding a new license) or in case of a action.

It will appear between the menu and the content part on all MegaLog pages.

If a new QVP message appears an "eye catcher" starts as well for round about 30 seconds. You have to acknowledged each or all entry in the QVP.

The maximum length of the QVP is 8 lines. The rest is not access able as long as the other messages are not acknowledged.

All management consoles on all workstations will see the same information, but only one needs to acknowledge it.

All QVP messages are deleted automatically after 7 days thru the DBM service.

In case of too many QVP messages to acknowledge you can use table help function under Config / Tables.

Appendix

Filter Language

The built in filter script language is optimized for speed and performance. Because of this you have to take care about the strict syntax:

- one command per line only
- don’t embed a command in command
- all commands and values are case sensitive
- general syntax for any command is “Command()”
- all parameters inside the brackets are separated by comma, e.g. move(a, b)
- all values needs to be in quotes, e.g. move(a, "1024")
- if you move values from one variable to one other, you don't have to convert it as long as it fits in the variable definition range! E.g. String "12.345" can be assigned to any float variable
- you can use leading spaces to visualize if/else levels

The tool “FilterLanguage.exe” will help you to develop filters scripts.

Filter Variable Types

The following variable types are available in the filter language:

- char
- string
- int8
- int16
- int32
- int64
- float
- datetime

Event Message Field

The following event message fields are access able by the filter scripts (Read and Write).

- datetime as datetime
- facility as int8
- level as int8
- hostname as string, max length 255
- appname as string, max length 48
- progid as string, max length 128
- msgid as string, max length 32
- user as string, max length 64
- message as string, max length 4000
- sdtime as string, max length 128
- sdorigin as string, max length 128
- sdmeta as string, max length 128
- sdother as string, max length 128
- url as string, max length 128
- fwevent as string, max length 64
- fwsourceip as int64
- fwsourceport as int16
- fwprotocol as int8
- fwdestinationip as int64
- fwdestinationport as int16
- eventdeletiondate as datetime

Filter Commands

Remarks

Command	*****	
Example	* This is a remark * **********and this ******** ** this as well	If the line starts with "*" the line will be interpreted as comment.

Define Variables

Command	**Var(var-type, var-name)**	
Parameter 1	Filter variable type	See "Appendix: Filter Variable Types"
Parameter 2	Variable name	Any name, but not the reserved keywords in list "Appendix: Event Message Field"

Example	var(string, s) var(int8, a)	Per default the following values are assigned to the variables: char, string = " " int8, int16, int32, int64, float = "0" datetime = "01-01-2000 00:00:00"

Move Values

Command	**move(var-to, var-from)**	
Parameter 1	Variable or event message field name	
Parameter 2	Variable, event message field name or value	
Example	move(a, "99") move(a, b) move(classification, "-none-")	You don't have to convert values, this happens automatically as long as it fits in the definition of the destination variable. E.g. var(string, s) var(float, f) move(s, "1.223") move(f, s)

Find Functions

Command	**findipstring(var-from, var-selector, var-to)**	
Parameter 1	Variable or event message field name	String
Parameter 2	Variable, event message field name or value	String
Parameter 3	Variable or event message field name	String
Example	message = "… outside=1.2.3.4/23 …"" findipstring(message, "outside=", a)	This function finds the given substring and expect directly behind an IP address. This will be copied as string to the var-to. In case off an error "0.0.0.0" is written to var-to.

Command	**findport(var-from, var-selector, var-to)**	
Parameter 1	Variable or event message field name	String
Parameter 2	Variable, event message field name or value	String
Parameter 3	Variable or event message field name	Number

Example	message = "… port=12345 …"" findport(message, "port=", a)	This function finds the given substring and expect directly behind an port. This will be copied as number to the var-to. In case off an error "0" is written to var-to.

Command	**findipport(var-from, var-counter, var-to-ip, var-to-port)**	
Parameter 1	Variable or event message field name	String
Parameter 2	Variable, event message field name or value	Int32
Parameter 3	Variable or event message field name	Int64
Parameter 4	Variable or event message field name	Int16
Example	findipport(message, "1", fwsourceip, fwsourceport)	This function finds the X occurrence of an IP address/port combinations. The separation sign between address and port needs to to ":" or "/". Then it stores the IP address as int64 in var-to-ip and the port number as int16 in var-to-port. In case of an error the destination var kept untouched.

Command	**findprotocol(var-from, var-separator, var-to)**	
Parameter 1	Variable or event message field name	String
Parameter 2	Variable, event message field name or value	String
Parameter 3	Variable or event message field name	Int16
Example	findprotocol(message, " ", fwprotocol)	This function finds the X occurrence of well known port name strings. The separation sign between the strings can be defined in the second parameter. Then it stores the port number in var-to. In case of an error the destination var kept untouched.

Command	**findpos(var-from, var-selector, var-counter, var-to)**	
Parameter 1	Variable or event message field name	String
Parameter 2	Variable, event message field name or value	String

Parameter 3	Variable, event message field name or value	Int16
Parameter 4	Variable or event message field name	Int32
Example	findpos(message, ":", "2", a)	This function finds the X (parameter 3) occurrence of string (parameter 2). Then it returns the position to var-to. In case of an error the destination var kept untouched.

String Manipulations

Command	**upper(var)**	
Parameter 1	Variable or event message field name	String
Example	var(string, s) move(s, "hello") upper(s) ==> s = "HELLO"	This function converts the given string to upper case and returns it in the same variable.

Command	**lower(var)**	
Parameter 1	Variable or event message field name	String
Example	var(string, s) move(s, "Hello") lower(s) ==> s = "hello"	This function converts the given string to lower case and returns it in the same variable.

Command	**trim(var, val-trim)**	
Parameter 1	Variable or event message field name	String
Parameter 2	Variable or event message field name	String
Example	var(string, s) move(s, "hhhellohhh") trim(s, "h") ==> s = "ello"	This function trims the given string from val-trim value (parameter 2) and returns it in the same var (parameter 1).

Command	**splitstring(var-from, var-selector, var-counter, var-to)**	
Parameter 1	Variable or event message field name	String

Parameter 2	Variable, event message field name or value	String
Parameter 3	Variable, event message field name or value	Int32
Parameter 4	Variable or event message field name	String
Example	splitstring(message, " ", "3", s)	This function finds the X substring (parameter3), separated by var-selector and returns the string in var-to. In case of an error it returns "".

Command	**substring(var-from, var-position, var-length, var-to)**	
Parameter 1	Variable or event message field name	String
Parameter 2	Variable, event message field name or value	Int32
Parameter 3	Variable, event message field name or value	Int32
Parameter 4	Variable or event message field name	String
Example	splitstring(message, "10", "5", s) splitstring(message, "10", "9999", s) just copies from 10 to the end of message	This function copies the substring starting at position var-position (parameter 2) with the length var-length (parameter 3) and returns the string in var-to. No error will happen when the position or length extend the original string, the return value will be then "".

Calculations

Command	**add(var-to, var-1, var-2)**	
Parameter 1	Variable or event message field name	Number
Parameter 2	Variable, event message field name or value	Number
Parameter 3	Variable, event message field name or value	Number
Example	add(a, a, "1") add(a, b, c)	This function sums up var-1 (parameter 2) and var-2 (parameter 3) and returns it in var-to (parameter 1).

Command	**minus(var-to, var-1, var-2)**

Parameter 1	Variable or event message field name	Number
Parameter 2	Variable, event message field name or value	Number
Parameter 3	Variable, event message field name or value	Number
Example	minus(a, a, "1") minus(a, b, c)	This function subtracts var-2 (parameter 3) from var-1 (parameter 2) and returns it in var-to (parameter 1).

Conversions

Command	**stringtoip(var-to, var-from)**	
Parameter 1	Variable or event message field name	Int64
Parameter 2	Variable, event message field name or value	String
Example	stringtoip(hostip,"127.0.0.1")	This function converts an IP address string into int64 for event messages field. In case of an error it returns "0".

Command	**iptostring(var-to, var-from)**	
Parameter 1	Variable or event message field name	String
Parameter 2	Variable, event message field name or value	Int64
Example	iptostring(s, hostip)	This function converts an IP address integer field like event messages field to a string. In case of an error it returns "0.0.0.0".

Command	**protocoltono(var-to, var-from)**	
Parameter 1	Variable or event message field name	String
Parameter 2	Variable, event message field name or value	Int16
Example	protocoltono(a, "upd")	This function converts a protocol name to the defined protocol number and returns it in var-to. In case on an error the return value is "-1".

Command	notoprotocol(var-to, var-from)	
Parameter 1	Variable or event message field name	Int16
Parameter 2	Variable, event message field name or value	String
Example	notoprotocol(s, fwprotocol”)	This function converts a protocol number to the defined protocol string and returns it in var-to. In case on an error the return value is “-”.

DateTime Functions

Command	now(var, UTC)	
Parameter 1	Variable or event message field name	Datetime
Parameter 2	true | false	true or false for UTC (true = UTC, false = LT)
Example	var(datetime, dt) now(dt, true)	This function provides the current date and time in UTC or LT to var.

Command	date(var, UTC)	
Parameter 1	Variable or event message field name	String
Parameter 2	true | false	true or false for UTC (true = UTC, false = LT)
Example	date(s, true)	This function provides the current date as string in UTC or LT to var.

Command	time(var, UTC)	
Parameter 1	Variable or event message field name	String
Parameter 2	true | false	true or false for UTC (true = UTC, false = LT)
Example	time(s, true)	This function provides the current time as string in UTC or LT to var.

Command	year(var, UTC)	
Parameter 1	Variable or event message field name	Int32

Parameter 2	true | false	true or false for UTC (true = UTC, false = LT)
Example	year(a, true)	This function provides the current year as number and returns it in var.

Command	**month(var, UTC)**	
Parameter 1	Variable or event message field name	Int32
Parameter 2	true | false	true or false for UTC (true = UTC, false = LT)
Example	month(a, true)	This function provides the current month as number and returns it in var.

Command	**day(var, UTC)**	
Parameter 1	Variable or event message field name	Int32
Parameter 2	true | false	true or false for UTC (true = UTC, false = LT)
Example	day(a, true)	This function provides the current day-date as number and returns it in var.

Command	**hour(var, UTC)**	
Parameter 1	Variable or event message field name	Int32
Parameter 2	true | false	true or false for UTC (true = UTC, false = LT)
Example	hour(a, true)	This function provides the current hour as number and returns it in var.

Command	**minute(var, UTC)**	
Parameter 1	Variable or event message field name	Int32
Parameter 2	true | false	true or false for UTC (true = UTC, false = LT)
Example	minute(a, true)	This function provides the current minute as number and returns it in var.

Command	second(var, UTC)	
Parameter 1	Variable or event message field name	Int32
Parameter 2	true | false	true or false for UTC (true = UTC, false = LT)
Example	second(a, true)	This function provides the current second as number and returns it in var.

If-Else

Command	if(var-1, compare-sign, var-2) { } else { }	
Parameter 1	Variable or event message field name	**String**
Parameter 2	Compare symbols	= != in
Parameter 3	Variable or event message field name	String

Example	if(s1, in, "A;B;C;D;E;F")
	{
	exit(true)
	}
	else
	{
	exit(false)
	}
		This function compares two strings (= or !=)and branch to true or false {}.
		
		In case of the compare symbol "in" the function compares the string 1 in the array of string 2. The values need to be separated by ";" Starting and ending spaces are ignored.

Command	if(var-1, compare-sign, var-2) { } else { }	
Parameter 1	Variable or event message field name	**Number**
Parameter 2	Compare symbols	> < >= <= = !=
Parameter 3	Variable or event message field name	Number

Example	if(a1, <, a2)
	{
	exit(true)
	}
	else
	{
	exit(false)
	}
		This function compares two numbers and branch to true or false {}.

Return Values

<table>
<tr><td>Command</td><td colspan="2">exit(0 | 1)</td></tr>
<tr><td>Parameter 1</td><td>true | false</td><td>Value true or false</td></tr>
<tr><td>Example</td><td>exit(true)</td><td>If a filter process returns true the event message will pass the TLPP and RTV filters. In case of an action filter value true will cause an action.
<table><tr><th>Return Value</th><th>true</th><th>false</th></tr><tr><td>TLPP Agent Filter</td><td>pass-</td><td>drop event</td></tr><tr><td>TLPP Group Filter</td><td>pass-</td><td>drop event</td></tr><tr><td>Action Filter</td><td>start-</td><td>no action</td></tr><tr><td>RTV Filter</td><td>pass-</td><td>drop event</td></tr></table></td></tr>
</table>

Filter Example

The following example is a filter script for a TLPP module. It inspects the Syslog data stream and analyse it in case the source was a Cisco ASA 55xx or Cisco PIX 5xx.

```
1   ** process only if source is ASA or PIX
2   var(string, cisco)
3   substring(message, "0", "4", cisco)
4   if(cisco, in, "%PIX;%ASA")
5   {
6     * find message-id
7     var(string, s)
8     splitstring(message, " ", "0", s)
9     trim(s, "%")
10    trim(s, ":")
11    move(fwevent, s)
12    splitstring(s, "-", "2", msgid)
13
14    * find protocol
15    findprotocol(message, " ", fwprotocol)
16
17    * find source/destination ip/port
18    findipport(message, "1", fwsourceip, fwsourceport)
19    findipport(message, "2", fwdestinationip, fwdestinationport)
20  }
21  exit(true)
```

a) ASA or PIX adds a prefix to the message always. In the line 2 – 4 the filter looks for this prefix. If the prefix is not found then the filter process will end in line 20.

b) If the one of tags where found the filter starts to analyse it for …

c) … the message code (line 6 – 11) and stores it in the event message field "fwevent"."

d) In line 12 only the number code is separated and stored in event message field "messageid".

e) Then it looks for the protocol and stores this information in "fwprotocol" (line 15).

f) Then it looks for the first IP address/port combination, assumes it is the source and stores it in "fwsourceip" and "fwsourceport" (line 18).

g) Then it looks for the second IP address/port combination, assumes it is the destination and stores it in "fwdestinationip" and "fwdestinationport" (line 19).

Facility Definitions

0	=	Kernel
1	=	User
2	=	Mail
3	=	Daemon
4	=	Auth
5	=	Syslog
6	=	Lpr
7	=	News
8	=	UUCP
9	=	Cron
10	=	System0
11	=	System1
12	=	System2
13	=	System3
14	=	System4
15	=	System5
16	=	Local0
17	=	Local1
18	=	Local2
19	=	Local3
20	=	Local4
21	=	Local5
22	=	Local6
23	=	Local7

Severity/Priority Definitions

The Syslog severity/priority colour code legends is always access able on the right side of the main menu. Move the mouse pointer over the symbols and a tooltip will appear.

0	=	Emergency
1	=	Alert
2	=	Critical
3	=	Error
4	=	Warning
5	=	Notice
6	=	Info
7	=	Debug

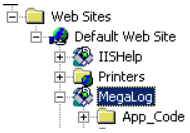
Access Security

IIS and access to MegaLog pages

In general Syslog event are not secret information, so read access should not be problem. Nevertheless MegaLog administrator is able to manipulate and set filter scripts to influence the Syslog traffic. Because of this it is import to have the possibility to limit the access to the administrative pages for single users or groups.

MegaLog TP is based on Microsoft's Internet Information Service (IIS) because on the need of a .NET framework. To increase the application security (e.g. prevent standard users to access administrative pages) IIS is able to control this.

We suggest first to allow anonymous access to all pages on level "MegaLog" properties.



Because of this all Java Applets will start without asking for user/password.

Now decide what pages needs protection. We suggest to limit access for the following pages to the main administrator:

- ActionFilterDef.aspx
- Actions.aspx
- DBConfig.aspx
- FilterDetails.aspx
- Hosts.aspx
- Licensing.aspx
- ModErrors.aspx
- RTVFilterDef.aspx
- Sounds.aspx
- TableHelper.aspx
- TLPPAgents.aspx
- TLPPFilterDef.aspx
- TLPPTypes.aspx
- TMConfig.aspx

Limit the access of the dedicated pages to "Integrated Windows authentication" and remove "anonymous access".

SQL Database

All information event and configuration is stored in one SQL database. Perhaps you want to increase the security of the database because of:

- to use not the same connection string for TM, DBM and TP
- not work with database top user account “sa” or "Trusted User"

The window services and modules need different access rights to the SQL database. The following table will help you to establish the most secure variant for you environment.

MySQL:

If you installed MegaLog in a MySQL environment, the users mgu_TM, mgu_DBM and mgu_TP are created automatically (mgu_TM and mgu_TP are used from the beginning on, mgu_DBM needs to be set up after the service created the database in the config file.)

MSSQL:

If you installed MegaLog in a MSSQL environment, only the user mgu_TP is created and configure to use by the module TP. We suppose that the modules TM and DBM are running on a server/workstation inside a MS domain. Because of this the installation configure automatically "SSPI=true" for "Trusted User" System/Network-Service. If the services/module are not running within the same MS domain you have to use connection strings with user-id and password.

SQL Table	**Module TLPP**	**Module TM** (Use MySQL user "mgu_TM")	**Module DBM** (Use MySQL user "mgu_DBM")	**Module TP** (Use MSSQL and MySQL user "mgu_TP")
ActionFilterDefinitions	-	S	-	S / I / U / D
Actions	-	S	-	S / I / U / D
DBMaintanance	-	S	S / U	S / U
Events	-	I	S / D	S
Query	-	-	-	S / I / U / D
EventStatisticsByDay/-Hour/-Min	-	S / I / U / D	S / I / U / D	S
FilterDetails	-	S	-	S / I / U / D
Hosts	-	S / I / U / D	S / I / U / D	S / U / D
ModuleErrors	-	S / I / U / D	S / I / U / D	S / I / U / D
ModuleInfo	-	S / I / U / D	S / I / U / D	S / I / U / D
Ports	-	-	-	S
Protocols	-	-	-	S
QVP6	-	S / I / U / D	S / I / U / D	S / U / D
RTVFilterDefinitions	-	S	-	S / I / U
Sounds	-	-	-	S / I / U / D
TLPPFilterDefinitions	-	S / I / U / D	-	S / I / U / D
TLPPGroups	-	S	-	S / I / U / D
TLPPs	-	S / U	-	S / I / U / D
TLPPTypes	-	S	-	S / I / U / D
TMConfig	-	S / U	-	S / U

S = Select
I = Insert
U = Update
D = Delete

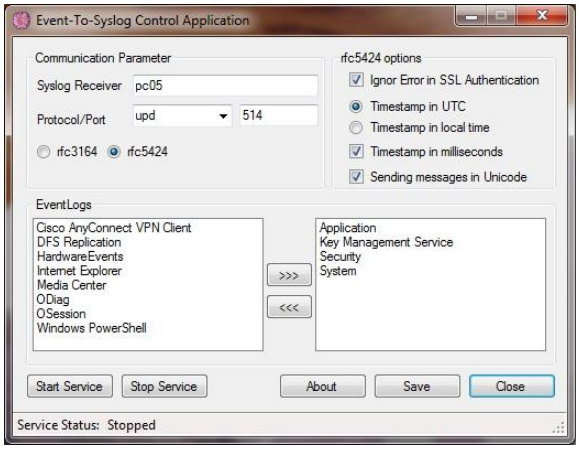
Please have a look to the yellow marked row. There you can see that only module TM is allowed to insert events.

The module DBM is the only module with sufficient rights to delete events.

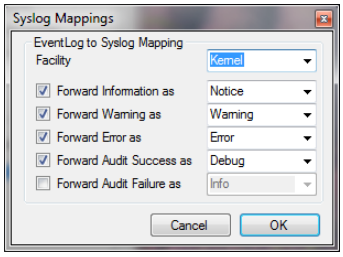
Per default the module TP cannot delete events!

Retrieving Windows Event-Log Messages

The Windows service Event-To-Syslog collects, converts and send Windows event log entries to a Syslog server. This program need to be installed on all Windows servers and workstation from where you want to get the event log entries to the central Syslog server.



Bundled with the service comes a control application.



Here you can select what event logs are observed and how the event severity types are mapped to the Syslog severity types.

Beside the function to transmit the data either in the old Syslog format (rfc3164) or in the new format (rfc5424), the generated timestamp can be in 1/1000 second. This is presently a unique function because windows event log entries are stored only with a second resolution. If you select "Timestamp in millisecond" the service will add this fraction of time to every single event.

After saving your configuration you can stop and start the service immediately. Nevertheless the service detects a configuration change within on minute and apply them automatically.

Retrieving Linux/Unix System Log Messages

The majority of Linux and Unix systems are using Syslog or Syslog-ng for collecting local messages. This service is able to forward events via Syslog protocol to other Syslog instances; as well you can use this function to forward the messages to a central Syslog server. In case of a MegaLog installation the traffic will be forwarded to a TLPP.

Syslog Demon

Please add the following coloured line /etc/syslog.conf config file.

```
# /etc/syslog.conf - Configuration file for syslogd(8)
#
# For info about the format of this file, see "man syslog.conf".
#


#
#
# print most on tty10 and on the xconsole pipe
#
kern.warning;*.err;authpriv.none        /dev/tty10
kern.warning;*.err;authpriv.none       |/dev/xconsole
*.emerg                         *

# enable this, if you want that root is informed
# immediately, e.g. of logins
#*.alert                        root

*.*                             @2.2.2.2

...
```

Please change server IP address to the running TLPP from 2.2.2.2 to you real TLPP address.

After adding/changing the line to the config file you have to restart the service to bring the new configuration to live.

/etc/init.s/syslog restart

Syslog-ng Demon

Please add the following coloured line /etc/syslog-ng/syslog-ng.conf config file.

```
...
filter f_newsnotice { level(notice) and facility(news); };
filter f_newscrit   { level(crit)   and facility(news); };
filter f_newserr    { level(err)    and facility(news); };
filter f_news       { facility(news); };

filter f_mailinfo   { level(info)      and facility(mail); };
filter f_mailwarn   { level(warn)      and facility(mail); };
filter f_mailerr    { level(err, crit) and facility(mail); };
filter f_mail       { facility(mail); };

filter f_cron       { facility(cron); };

filter f_local      { facility(local0, local1, local2, local3,
                          local4, local5, local6, local7); };

filter f_acpid      { match('^\[acpid\]:'); };
filter f_netmgm     { match('^NetworkManager:'); };

filter f_messages   { not facility(news, mail) and not filter(f_iptables); };
filter f_warn       { level(warn, err, crit) and not filter(f_iptables); };
filter f_alert      { level(alert); };

destination syslogserver { upd("2.2.2.2"); };
log { source(src); filter(f_warn); destination(syslogserver); };
log { source(src); filter(f_alert); destination(syslogserver); };
...
```

Please change server IP address to the running TLPP from 2.2.2.2 to you real TLPP address.

After adding/changing the lines to the config file you have to restart the service to bring the new configuration to live.

/etc/init.d/syslog-ng restart

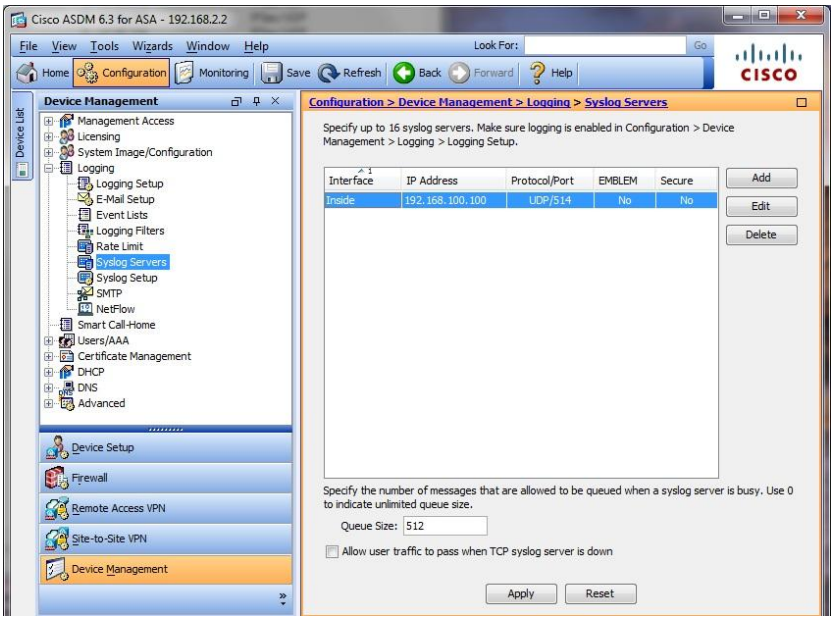
or *(it depends on your version)*

/etc/init.d/syslog restart

Retrieving CISCO PIX/ASA Syslog Messages

Cisco ASA

To enable Syslog messages from a CISCO ASA 55xx select first "Configuration", "Logging" and finally "Syslog Servers". Insert here a new Syslog server like TLPP from MegaLog. Don't forget to enable logging under "Logging Setup" and set the "Logging Filters" for "Syslog Servers" to e.g. "Severity: Warning".



Cisco PIX

The configuration for a CISCO PIX 5xx is similar to the CISCO ASA. First "Configuration", "Logging" and then "Syslog". Insert here a new Syslog server like TLPP from MegaLog. Don't forget to enable logging under "Logging Setup".