

op5 LogServer 3.5

Manual

Contents

Preface	V
1 Web Interface	1
1.1 Logging in	2
1.2 View	3
1.2.1 Search	4
1.2.1.1 Query language	5
1.2.1.2 Query builder	7
1.2.1.3 Search criteria	9
1.2.1.4 Save your search query	10
1.2.1.5 Search using a saved filter	11
1.2.1.6 Manage filters	12
1.2.1.7 Auto refresh	14
1.2.1.8 CSV export	14
1.2.2 Timeline browsing	15
1.2.2.1 Select date	15
1.2.2.2 Move in time	16
1.2.2.3 Import archived data	16
1.2.3 Search result	18
1.2.3.1 Modify view settings	18
1.3 Reports	20
1.3.1 Creating Auto reports	20
1.3.2 Auto Report Parameters	21
1.3.2.1 Report Name	21
1.3.2.2 Description	22
1.3.2.3 Search Filter	22
1.3.2.4 Recipient Type	22
1.3.2.5 Email Recipients or File Path	22
1.3.2.6 Generating Interval	22
1.3.3 Manage an Auto Report	23
1.3.3.1 Edit	23

1.3.3.2	Deleting	23
1.3.3.3	Send now	23
1.3.4	Summary reports	24
1.3.5	Creating global or private summary report	25
1.3.6	Manage a Global or Private summary Report	26
1.3.6.1	Deleting	26
1.3.6.2	Viewing	27
1.4	Settings	28
1.4.0.3	Database Storage	29
1.4.0.4	Local Storage	30
1.4.0.5	Remote Storage	31
1.4.1	Enable fulltext index	31
1.4.2	The monitor host	31
1.4.3	Use Ninja	32
1.4.4	Host information page	32
1.4.5	Import filter	33
1.4.6	Export filters	33
1.5	Users and Groups	34
1.5.1	User Management	34
1.5.1.1	Add User	34
1.5.1.2	Edit User	35
1.5.1.3	Delete User	35
1.5.1.4	Changing password as user	35
1.5.2	Group Management	36
1.5.2.1	Default Groups	36
1.5.2.2	Add Group	37
1.5.2.3	Edit Group	37
1.5.2.4	Delete Group	37
1.5.3	Audit tracking	38
2	Configuring Clients	39
2.1	Windows Machines	39
2.2	UNIX Machines	40
2.2.1	syslogd	40
2.2.2	syslog-ng	41
2.2.3	Sending Text Files to LogServer	42
2.3	Other Equipment	42

3 op5 LogServer Technology	43
3.1 The Syslog Protocol and Implementations	43
3.1.1 Usage	43
3.2 op5 LogServer components	44
3.3 LogServer Storage	45
3.3.1 The PostgreSQL database	45
3.3.2 Local Storage	45
3.3.3 Remote Storage	45
A Installation	46
A.1 Basic Installation	46
A.2 Installing LogServer	46
A.2.1 Obtaining tar.gz files	47
A.3 Updating	47
A.4 Upgrading	48
B Using Remote Storage	49
B.1 Mounting a Windows Fileserver	50
B.2 Mounting an NFS share	50
C Workflow	51
C.1 Connector	52
C.2 Rotate	52
D Advanced DB Management	53

Preface

Modern organisations have higher demands to secure their IT environment than just a few years ago – for many reasons:

- they store credit card information
- because of legislation
- because of demands on public service organisations
- Securing high quality towards your customers

This makes op5 LogServer an increasingly important part of many organisations' IT systems.

Virtually every modern computer application logs what happens, and you can not know in advance which information will be important or not.

The syslog protocol, an important part of the LogServer architecture, provides a business standard for how to transfer data.

LogServer is unique in it's design and flexibility for storing large volumes of data, and accessing archived data is very easy.

It is our hope that your organisation will benefit from using LogServer on many levels, and that this manual will answer your questions quickly and to the point. If you have any queries about this manual, please send these to support@op5.com or call +46-31-7740924.

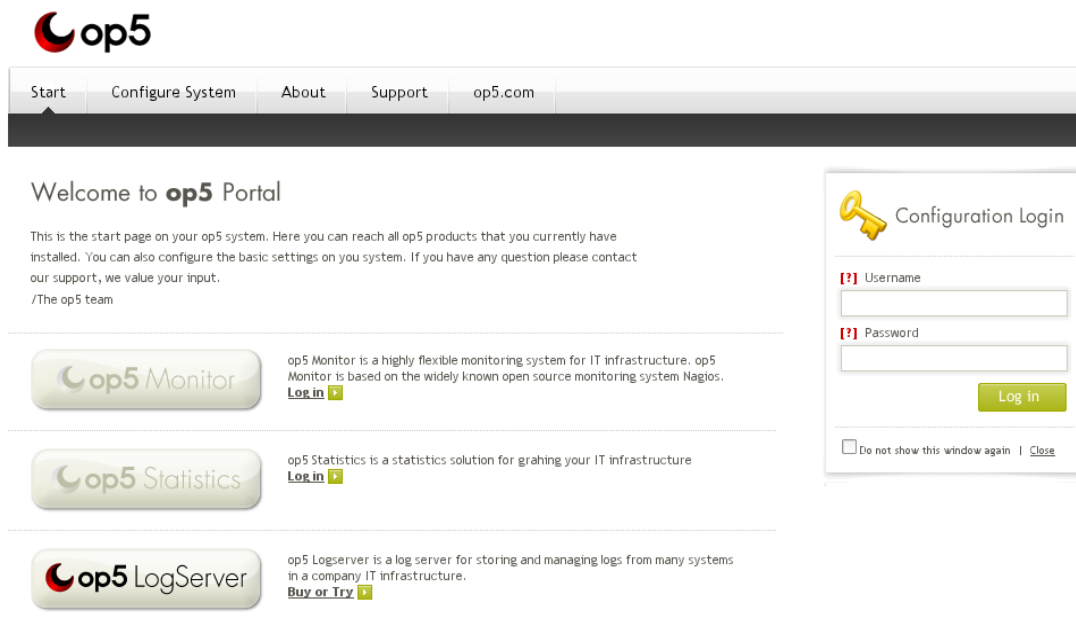
Chapter 1

Web Interface

Most operations you perform on your op5 LogServer is done from the web interface, including configuration.

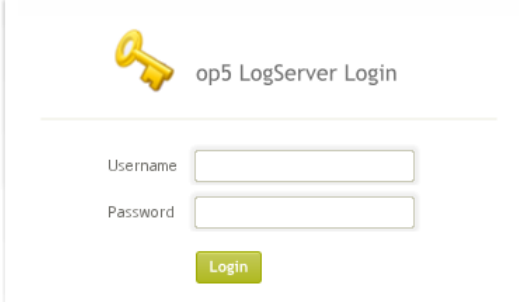
The web interface is intuitive, and you will find a clickable question mark near many options, where you can find context-related help.

If you need information about a specific option, you should look at context-related help-popups. If you need information about how to solve a specific task, this manual is the right place to look.



1.1 Logging in

Point your web browser to the server you installed LogServer on.

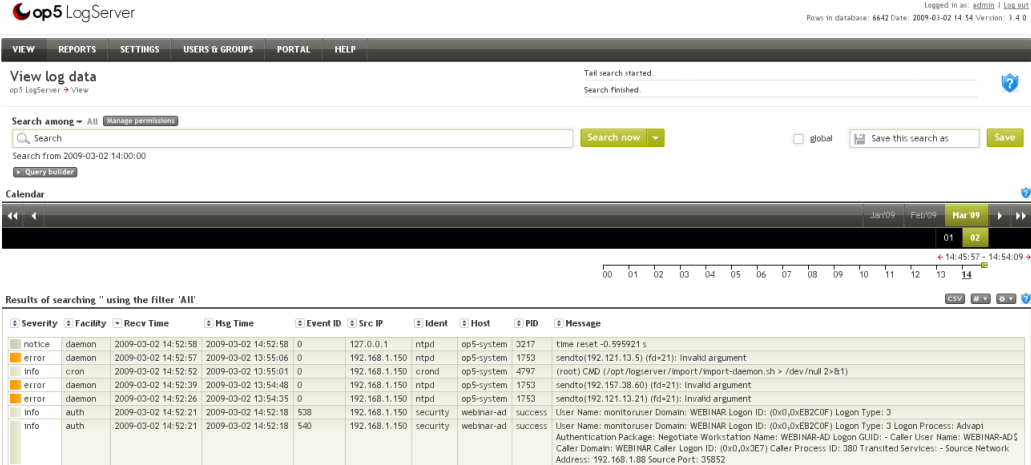
The image shows a web login interface for op5 LogServer. At the top left is a yellow key icon. To its right is the text "op5 LogServer Login". Below this, there are two input fields: "Username" and "Password". Below the "Password" field is a green "Login" button.

To log in, fill out your user name and password and click the login button.

User name	Password	Description
admin	admin	Administrator privileges

You should log in as admin and create users and passwords that suit your needs.

1.2 View



op5 LogServer

Logged in as: admin | Logout
Rows in database: 6642 Date: 2009-03-02 14:54 Version: 3.4.0

VIEW REPORTS SETTINGS USERS & GROUPS PORTAL HELP

View log data
op5 LogServer > View

Tail search started.
Search finished.

Search among: All (Manage permissions)

Search
Search from 2009-03-02 14:00:00
Query builder

Search now Save this search as Save

global

Calendar

Jan 09 Feb 09 Mar 09

01 02

14:45:57 - 14:54:09

Results of searching " using the filter 'All'

Severity	Facility	Recv Time	Msg Time	Event ID	Src IP	Ident	Host	PID	Message
notice	daemon	2009-03-02 14:52:58	2009-03-02 14:52:58	0	127.0.0.1	ntpd	op5-system	3217	time reset -0.595921 s
error	daemon	2009-03-02 14:52:57	2009-03-02 13:55:06	0	192.168.1.150	ntpd	op5-system	1753	sendto(192.121.13.5) (fd=21): Invalid argument
info	cron	2009-03-02 14:52:52	2009-03-02 13:55:01	0	192.168.1.150	cron	op5-system	4797	(root) CMD: /opt/LogServer/Import/Import-daemon.sh > /dev/null 2>&1)
error	daemon	2009-03-02 14:52:39	2009-03-02 13:54:48	0	192.168.1.150	ntpd	op5-system	1753	sendto(192.157.38.40) (fd=21): Invalid argument
error	daemon	2009-03-02 14:52:26	2009-03-02 13:54:35	0	192.168.1.150	ntpd	op5-system	1753	sendto(192.121.13.21) (fd=21): Invalid argument
info	auth	2009-03-02 14:52:21	2009-03-02 14:52:18	538	192.168.1.150	security	webinar-ad	success	User Name: monitoruser Domain: WEBINAR Logon ID: (0x0,0xEB2C0F) Logon Type: 3 Logon Process: Advapi
info	auth	2009-03-02 14:52:21	2009-03-02 14:52:18	540	192.168.1.150	security	webinar-ad	success	Authentication Package: Negotiate Workstation Name: WEBINAR-AD Logon GUID: - Caller User Name: WEBINAR-AD\$ Caller Domain: WEBINAR Caller Logon ID: (0x0,0x3E7) Caller Process ID: 380 Transmitted Services: - Source Network Address: 192.168.1.88 Source Port: 35852

This is the first page you get to when you log in. The page is divided into 3 sections.

- Search ([1.2.1](#))
- Timeline ([1.2.2](#))
- Search result ([1.2.3](#))

When you click on View you will see the default 75 last received messages.

1.2.1 Search

To search for a message, simply type your search phrase in the search form box and press enter. You will then do a search in the full-text search index table in the database.

Both the result table and the timebar are updated when each hour of data are searched through in the database.

If you want to stop the search just click on "Stop" just below the search text field.

A Full-text search searches in all fields of the database for words you type in. Example: search of "connect" instead of msg="connect" will be searched in all text fields, taking more resources from the server.

If you want to define a more advanced search query you can use the op5 LogServer query language.

1.2.1.1 Query language

In op5 LogServer 3.0 we introduced a new Query Language to be able to do more complex searches.

Query Language

column	query	descriptor
Severity	sev severity	(=)
Facility	fac facility	(=)
Event ID	event event_id eventid	(=)
Src IP	ip src_ip source_ip sourceip	(=) (:) (~)
Ident	ident	(=) (:) (~)
Host	host	(=) (:) (~)
PID	pid	(=)
Message	msg message	(=) (:) (~)

Description of the descriptors:

- = means 'contains'
- : means 'starts with'
- ~ means 'matches regular expression'

For more info about PostgreSQL Regular Expression see [PostgreSQL Manual](#)

Examples:

```
msg="connection"
```

will search for any message including the string "connection"

```
sev=(warn info) -(statistics daemon) -msg:Log -ident=sshd
```

Logs that have severity "warn" or "info",

and do not contain words "statistics" or "daemon" in any field,

and where field "msg" does not begin with "Log",

and that were not generated by "sshd"

```
host~"192.168.1.(97|158)" -msg~"^(root) CMD"
```

Match host 192.168.1.97 or 158 and messages not starting with '(root) CMD'

```
msg~"UserName:\x09([[:alnum:]]$_-)*[^$]"
```

Match msg that contains "UserName:<tab>username" and username does not end with \$

Available fields: sev, fac, event, ip, ident, host, pid, msg

Severities: emerg(ency), alert, crit(ical), err(or), warn(ing), notice, info, debug

Facilities: kernel, user, mail, daemon, auth, syslog, lpr, news, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, clock2, local0 to local7, mark

1.2.1.2 Query builder

In LogServer 3.2 we introduced a Query builder function to make it easy for users to build their custom filters.

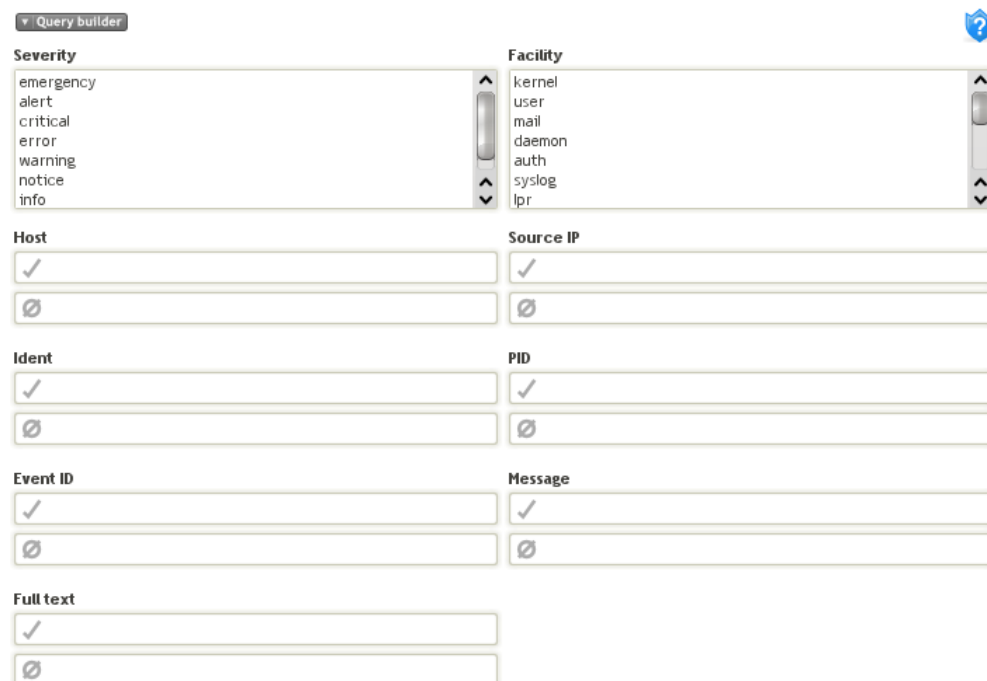
The Query Builder is bidirectional since op5 LogServer 3.3, meaning that it will expand your filter's criteria to the correct boxes when selecting a filter.

You can only get "OR" function in Query Builder

Enclose your text with "quotes"

Example: "User Name" "monitoruser"

Press the  located under the Search area to get a drop-down with options.



The Query builder interface is a form with a title bar "Query builder" and a help icon. It contains several sections for building a query:

- Severity**: A list box with options: emergency, alert, critical, error, warning, notice, info.
- Facility**: A list box with options: kernel, user, mail, daemon, auth, syslog, lpr.
- Host**: A text input field with a checkmark icon and a clear icon.
- Source IP**: A text input field with a checkmark icon and a clear icon.
- Ident**: A text input field with a checkmark icon and a clear icon.
- PID**: A text input field with a checkmark icon and a clear icon.
- Event ID**: A text input field with a checkmark icon and a clear icon.
- Message**: A text input field with a checkmark icon and a clear icon.
- Full text**: A text input field with a checkmark icon and a clear icon.

- To select more than one Severity or Facility, press and hold the Ctrl-key and click to select additional items.
- Enter the criteria you want to include in the search.

- Enter the criteria you want to exclude from the search.

Note: Regular expressions are not allowed in Query Builder.

1.2.1.3 Search criteria

When you create a search filter, you have several criteria to choose from. Some of these apply only to Windows and some only to UNIX.

Severity

Most UNIX daemons log their messages with more than one severity – depending on the message your database server might send a *notice* message or a *critical* message – or any of the other available messages.

Facility

This is the category of data. For instance: Your mail server daemons may log only using the mail facility and you will find most log on failures in the auth facility. This field is part of the syslog specification.

Host

The name of the logging host.

Source IP

Displays the IP-adress of the logging host.

Ident

This is normally the name of the logging application.

PID

This is normally the name of the logging application.

Event ID

This is only used by Windows hosts - it is the Event ID field from Windows Event Log.

Message

This is the actual log message. This is the field that is the least well defined. You may want to use this to exclude any messages that clutter your search results.

Full text

Use these fields to specify search criteria that should be applied to all fields.

1.2.1.4 Save your search query

The basic concept for using op5 LogServer is a *search filter*. Similar to any database search



- fill out a number of criteria in the Search area or use the Query builder ([1.2.1.2](#))
- decide if you want to make the filter Global (for everyone) or Local (for yourself)
- type a name for the filter in the Save this search as area
- click Save

The saved filter will be based on the one selected in "Search among".

1.2.1.5 Search using a saved filter

To be able to extend your search you can use an existing filter (saved search query).

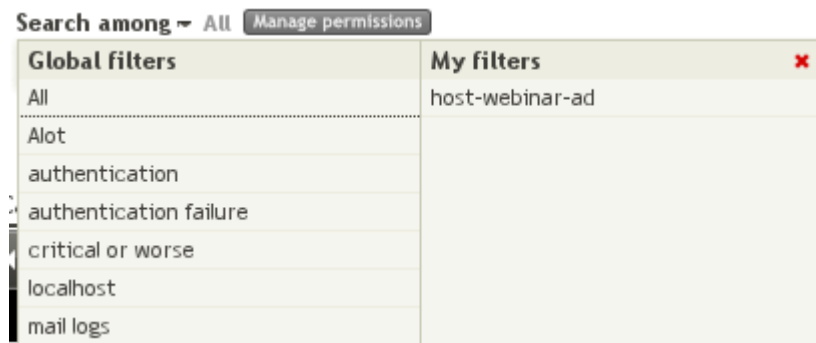
- Select the Filter you want to search within
- Enter your search criteria. You can use a simple full text search, the query language or the query builder.
- Press Search Now

The search will now use the criteria in the Filter and the criteria you typed in the Search field.

Since the filters are organised in a hierarchical data model (a tree-like structure) you can create multiple filters in multiple levels based on the same parent filter. Filters created from filters will become dependent on the filter out of which they were created.

1.2.1.6 Manage filters

The user management in LogServer supports making filters Global or Private (My filters) and assigning special permissions to the filters.



Delete filter

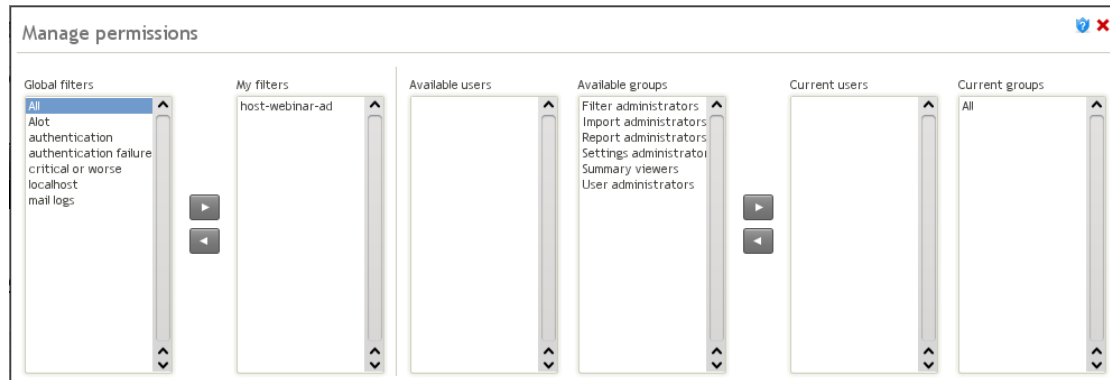
To delete a filter, select it from the filter dropdown menu and press **Remove**. **Note:** If you want to remove a filter that has other filters based on it you must first delete the "sub filters". Otherwise the "sub filters" are left unusable.

Edit filter


To view/edit the search criteria of an existing filter, select it from the filter dropdown menu and press **Edit**. You can now edit the search criteria directly in the search box or by using the Query builder. **Note:** A user can't edit Global filters unless they are member of the 'Filter administrators' group.

Global/Private filters

If you are member of 'Filter administrators' group you can view how your filter looks like and also change/assing permission to filters.



1.2.1.6.0.1 Global filters

To make a filter Global you mark it under My filters and press the .


- **Available Users/Groups:** Users/Groups you can grant permission to use the selected filter.
- **Current Users/Groups:** Users/Groups that have permission to use the selected filter.

Note: Making a filter global will also make all its parent filters global too.

Note: When you create/manage a filter, you need to decide which users should be able to use it. Default is none.

Note: If you want the filter to be visible for all users, use the 'All' group.

1.2.1.6.0.2 My filters

To make a filter My filters (Private) you mark it under Global and press the . Since it's a private filter no permissions can be applied.

Note: Making a filter private will make all its child filters private as well.

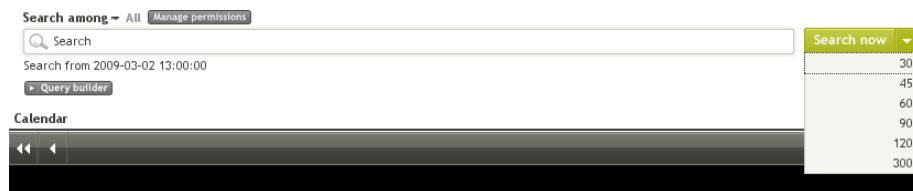
Note: Private filters are private, Filter administrators can't view your private filters.

1.2.1.7 Auto refresh

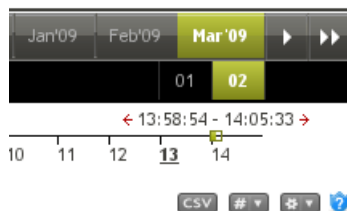
By clicking on the Down arrow on the Search now button will allow you to set a refresh period of the page. You can set it between 30 and 300 seconds.

The Auto refresh works like the UNIX program tail, showing the *last x messages*¹.

To cancel a refresh setting, click on cancel



1.2.1.8 CSV export



You can export the retrieved data in CSV format by clicking on **CSV**.

The format is a | (pipe) separated list.

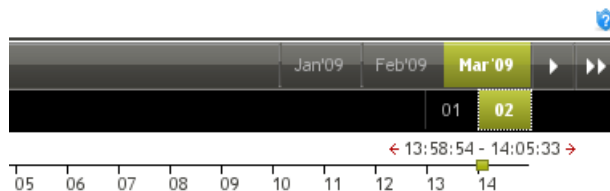
¹Depending of the user setting, see modify view settings [1.2.3.1](#)

1.2.2 Timeline browsing

You can move back and forth in time by using the timeline. If you go back in time and lack the data in the database you can easily import it (see section [1.2.2.3](#)).

1.2.2.1 Select date

To be able to browse/search on a specific day/hour you have to select it on the timeline.



- Select the month
- Select the date
- Select the hour you wish to display from.

The GUI will now display the *x messages*² matching the search criteria within the given time.

Messages are by default searched from the time you selected until the last message in database.

Example:

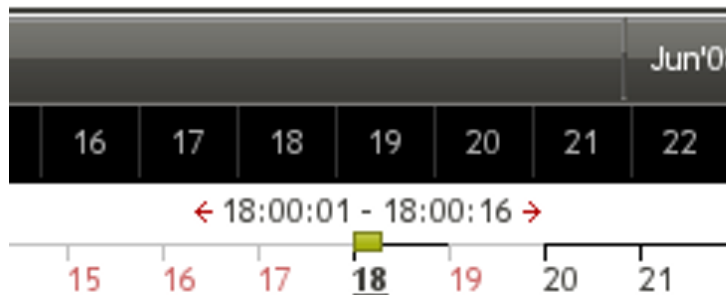
If you select 2008-07-24 hour 18, you will be able to search on all messages between 18:00 and the last message imported into the database.

Note: no-day-limit or unlimited search mode is deprecated, this is now the normal behavior.

²Depending of the user setting see modify view settings [1.2.3.1](#)

1.2.2.2 Move in time

To move in time you click the small red arrows, they will move in time and display the *X previous/following messages*³ matching the time in the timeline.

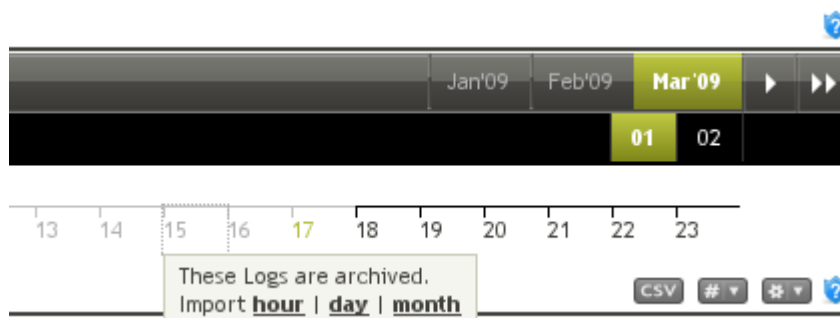


1.2.2.3 Import archived data

Data is kept in the database only for a limited amount of time,⁴ so that archived data does not occupy uncompressed disk space and slow down your searches.

However, the archived data is not discarded until after a much longer time. It is merely compressed and archived for possible future access.

When you have started an import it will continue in the background so you can always browse your messages.

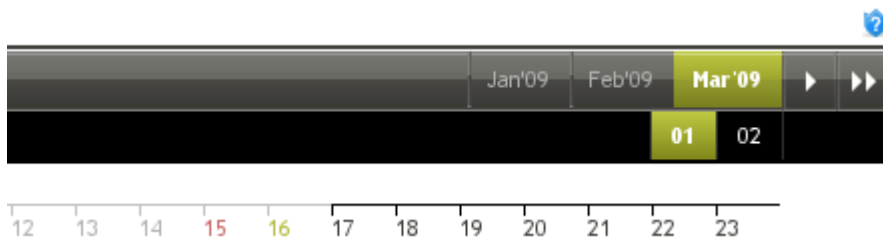


³Depending on the user settings, see modify view settings [1.2.3.1](#)

⁴See section [1.4](#) on page [28](#) for more information

To look into very old data:

- Select the date you want to import
- Choose hour/day/month to import



The import process will start to import the logs that correspond to your selection. A scrollbox will show the status of the import.

- A green hour number in the timeline indicate that it's being imported.
- A red hour number in the timeline indicate that something went wrong with the import.
- A black hour number in the timeline indicate that the import is done, the date will become white indicating that you have logs on that date.

Note: The import can take a lot of time depending on the amount of logs in your archive.

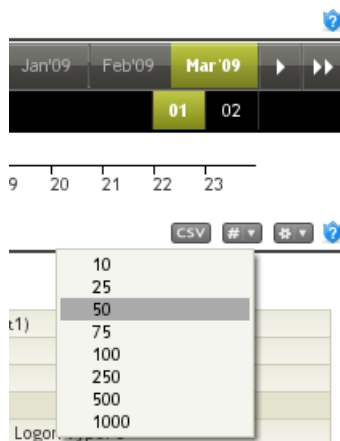
1.2.3 Search result


1.2.3.1 Modify view settings

You can change display settings. These settings will be resetted when logging out.

Number of rows returned

To select how many rows of data you want to be displayed.



- Click on 
- Select the number of rows you want to be displayed.

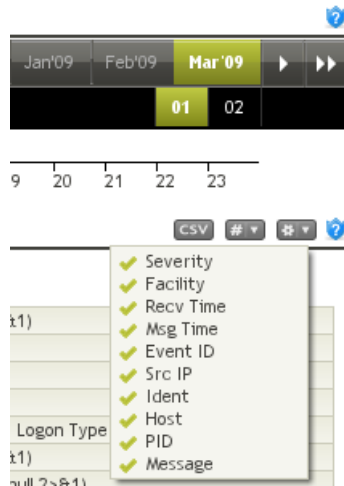
EventID


In the search result there is a column called EventID. If the log row contains a MS Windows Event the eventid is displayed as a link directly to www.eventids.net. If you click on the link you will be sent to the page for the eventid found in the log row.



Columns to display

To hide/unhide columns on the page.



- Click on 
- Check/Uncheck the field(s) you want to hide/unhide

1.3 Reports

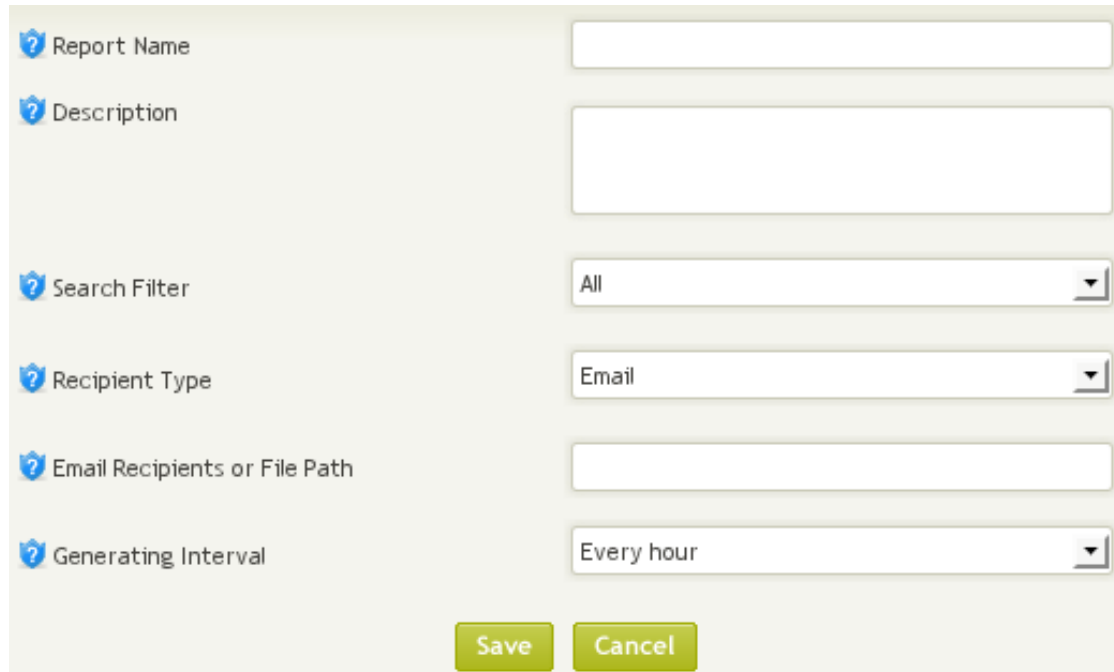
The reports section of LogServer has two main functions:

- Auto reports: Does scheduled searches and sends them to a list of users via e-mail or save them in a folder on your file server.
- Summary reports: Gives you top 10 hosts based on hits for each filter you have access to, and create graph (message per minute) for global/private filters.



1.3.1 Creating Auto reports

If you wish to create an Auto report – for instance you might want a log of failed password login attempts sent to you weekly – you should start by creating the appropriate search filter. See section [1.2.1.4](#) on page 10 for information on how to create filters.



If you have your search filter ready and wish to use it to create a report click REPORTS in the top menu and click Add new report.

- Create the appropriate search filter
- Click REPORTS in the top menu
- Click Create new report
- Fill out the parameters – see [1.3.2](#)

1.3.2 Auto Report Parameters

1.3.2.1 Report Name

This is the name of the report you are creating. Choose a name that is descriptive – not only for you but also for your colleagues. Sometimes it is a good idea to use your own name as part of the report, for future reference.

1.3.2.2 Description

Brief description of your report.

1.3.2.3 Search Filter

Choose your search filter from the menu.

1.3.2.4 Recipient Type

- Choose Email if you want the report to be sent via e-mail.
- Choose Path if you want the report to be created on a file server. You need to mount the file share on your LogServer server in order to have a local path.⁵

1.3.2.5 Email Recipients or File Path

Enter the email addresses that should receive the report (separated with comma ','), or the path in which it should be saved.

1.3.2.6 Generating Interval

Choose – Every hour, Every 6 hours, Every 12 hours, Daily, Weekly or Monthly – how often the report should be generated.

Click "Save" when you are done filling out the fields and then your report will be created.

⁵See section [B](#) on page [49](#) for information about mounting.

1.3.3 Manage an Auto Report


When you have created your report, it will show up every time you click REPORTS in the page top menu.



Auto reports	Summary reports - global	Summary reports - private	Add new report		
Recipient Type	Filter	Interval	Recipients	Report Name	Description
Email	authentication	Every hour	support@op5.com	hourly-authentications	 


1.3.3.1 Edit

To Edit a report

- Click on the  to the right of the auto report, or double click on the row in the list.
- Edit the fields you want to change and click on "Save".

1.3.3.2 Deleting

To Delete a report

- Click on the  to the right of the report
- Click OK on the popup

1.3.3.3 Send now

You can force a send of the selected report by clicking .

1.3.4 Summary reports

The global and private summary reports is used to:

- print graphs over how many logs matches a filter
- display statistics over top 10 hosts found with a filter

To be able to add or delete a report your user have to belong to the group 'Filter administrators'.

To view a report your user only have to belong to the 'Summary viewers' group.

1.3.5 Creating global or private summary report

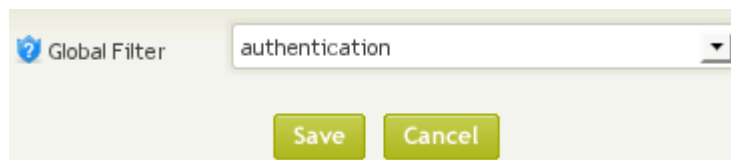
If you wish to create a global or private summary report – for instance you might want to view the number of hits for a filter matching incorrect ssh connections – you should start by creating the appropriate search filter. See section 1.2.1.4 on page 10 for information on how to create filters.

If you have your search filter ready and wish to use it to create a report click REPORTS in the top menu and click Add new report.

Summary report - global

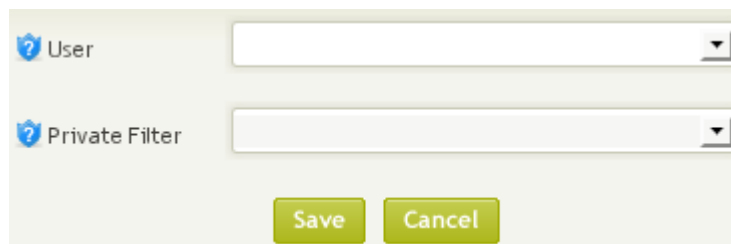
When you create global filter, summary reports for the global filter will be create automatically.

However if you delete your contact or upgrade you might have to create one manually.



A screenshot of the 'Global Filter' summary report form. It features a label 'Global Filter' with a question mark icon, a dropdown menu currently showing 'authentication', and two green buttons labeled 'Save' and 'Cancel' at the bottom.

Summary report - private



A screenshot of the 'Private Filter' summary report form. It contains two sections: 'User' with a dropdown menu and 'Private Filter' with another dropdown menu. Both dropdowns are currently empty. At the bottom are two green buttons labeled 'Save' and 'Cancel'.

- Choose user that the report should belong to.
- Choose what private filter you like to base the report on.
- Click on "Save" and your report is created.

Note: When you have added your report it will take maximum 5 minutes time to untill any graphs are created.


1.3.6 Manage a Global or Private summary Report

When you have created your report, it will show up every time you click REPORTS in the page top menu and then Global or Private summary reports flap.



1.3.6.1 Deleting

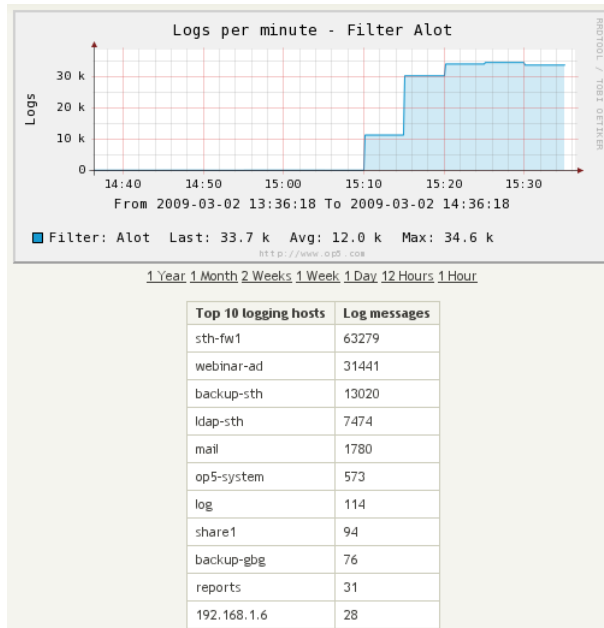
To Delete a report

- Click on the  to the right of the report
- Click OK on the popup

1.3.6.2 Viewing

To view a report click on the  to the right of the report.

You will then see a view like this:



The view is divided in to two parts:

- a graph displaying number of filter matches
- a Top 10 logging hosts table with number of matches per host.

You can "zoom" in on the graph by select what timeframe you want to look at by pressing the links under the graph image.

[1 Year](#) [1 Month](#) [2 Weeks](#) [1 Week](#) [1 Day](#) [12 Hours](#) [1 Hour](#)

1.4 Settings

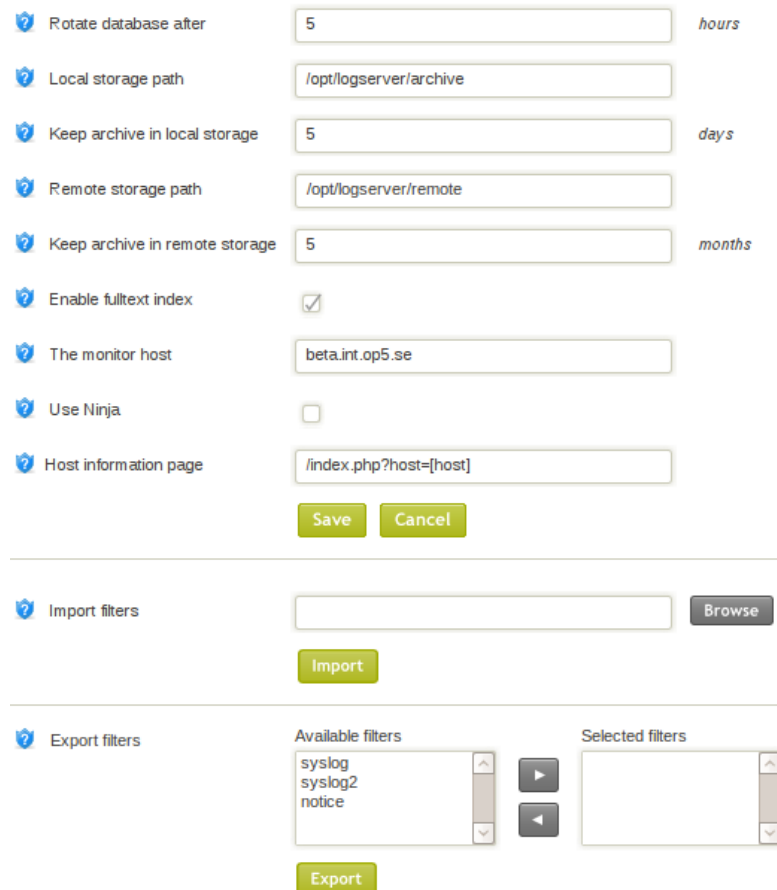
LogServer stores the logged data in three different locations:

- A local database for normal web access of latest data
- Compressed archive for longer term storage on local file system
- Compressed archive on remote file server for storage up to many years⁶

We recommend that you use op5 Monitor to check the available disk space on all disks used to store log data, so that you receive an alert if disk space is insufficient.

⁶The limit of the remote storage is only in amount of disk space available on the file server.

The picture below shows how the settings page looks like. Each option will be described in the next sections.



The screenshot displays the settings page for op5 LogServer. It features a list of configuration options, each with a help icon (question mark in a blue circle) and a text input field. The options are: 'Rotate database after' (set to 5, unit: hours), 'Local storage path' (set to /opt/logserver/archive), 'Keep archive in local storage' (set to 5, unit: days), 'Remote storage path' (set to /opt/logserver/remote), 'Keep archive in remote storage' (set to 5, unit: months), 'Enable fulltext index' (checked), 'The monitor host' (set to beta.int.op5.se), 'Use Ninja' (unchecked), and 'Host information page' (set to /index.php?host=[host]). Below these options are 'Save' and 'Cancel' buttons. A horizontal line separates this section from the 'Import filters' section, which has a text input field, a 'Browse' button, and an 'Import' button. Another horizontal line separates this from the 'Export filters' section, which shows 'Available filters' (syslog, syslog2, notice) and 'Selected filters' (empty) with arrows between them, and an 'Export' button.

Rotate database after	5	hours
Local storage path	/opt/logserver/archive	
Keep archive in local storage	5	days
Remote storage path	/opt/logserver/remote	
Keep archive in remote storage	5	months
Enable fulltext index	<input checked="" type="checkbox"/>	
The monitor host	beta.int.op5.se	
Use Ninja	<input type="checkbox"/>	
Host information page	/index.php?host=[host]	

Save Cancel

Import filters

Browse

Import

Export filters

Available filters

- syslog
- syslog2
- notice

Selected filters

Export

1.4.0.3 Database Storage

How long you wish to keep data in the database – the Rotate Database After setting – depends on how much data you log. Most organisations are happy with the default setting of 5 days, but if you log very much data you may need to store it for a shorter amount of time in regards to performance and disk space used.

Note: Old values will be converted if you upgrade.

1.4.0.4 Local Storage

The Local Storage Path is a setting you normally do not need to touch, unless you wish to save it on another storage unit.

The Keep archive in local storage setting with it's default of 5 days regulates for how long the data will be stored on disk on the LogServer machine. After this period of time, data will be stored only on the remote file server – still accessible but the access will be slower.

The issue is disk space; You would normally want to save data for as long as possible, without filling up the local hard disk. Keep in mind that since the amount of logged data per day often increases over time, you do need a lot of free disk space for the future.

Note: Old values will be converted if you upgrade.

1.4.0.5 Remote Storage

You should mount a remote file server in the file system on your LogServer server. You can read more about this in section [B](#) on page [49](#).

When you have done so, set the Remote Storage Path to the mount point – you can use `/opt/logserver/remote` or any other path you choose.

If you wish to impose a time limit on the remote storage, you can do so with the setting Keep Archive in Remote Storage.

Note: During upgrade Forever will be converted to 999 Months.

Note2: 999 Months is maximum limit.

1.4.1 Enable fulltext index

In some environments full text indexing of log messages is not really a good thing.

For example if you have a lot of log messages from a firewall that contains a lot of "non-words", binary data dumps and such.

Log messages like that can hog your CPU and affect the responsiveness of the op5 LogServer system.

Note: If you turn off the full text index, queries using full text syntax will still work but a bit slower.

1.4.2 The monitor host

Here you can define the hostname of your monitor server that will be used in the links in the host field in the search result.

1.4.3 Use Ninja

Check this check box to have the links in the host field in the search result pointing to the Ninja GUI instead of the standard Monitor GUI.

1.4.4 Host information page

If you like to have an custom URL, instead of the standard URL to Monitor for the link in the host field in the search result, you can define it here.

Note: You still need to define the hostname in the text field **The monitor host**.

This can be any URL and to have the hostname added to the URL just use a [host] like in this example:

/index.php?host=[host]

1.4.5 Import filter

You can import already exported filters here. Just click on Browse to chose the file. Then click on Import to import the filters.

Note: Every imported filter will be set as global with default permissions.

1.4.6 Export filters

Chose the filters you like to export and "move" them over from Available filters to Selected filters. Click on Export to save the XML file containing the filters. You can then import them via the Import filters section in Settings.

When exporting a filter that depends on an other filter both of them will be exported to make sure dependencies are untouched.

Note: Both global and private filters can be exported and no permission settings will be included.

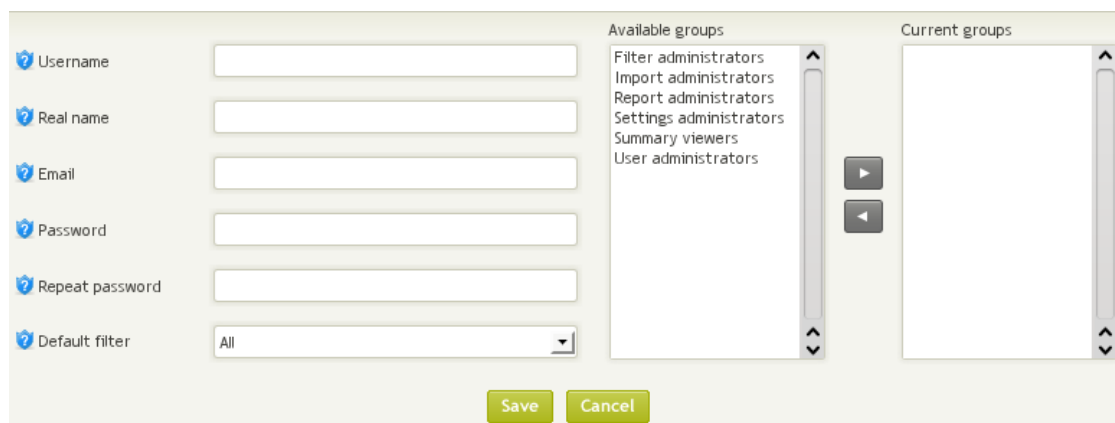
1.5 Users and Groups


To access Users and Groups, you have to be logged on as a user with admin privileges. If you have user administrator privileges, you will see a link Users and Groups in the main menu at the top.

1.5.1 User Management


1.5.1.1 Add User

To add a new user click on 



- Fill in Username
- Real Name
- Email
- Password
- Repeat password
- Select the group(s) you want the user to belong to
- Select default filter to be used for the user
- And press 

1.5.1.2 Edit User

- To edit a user, click on  or doubleclick on the row of the user.

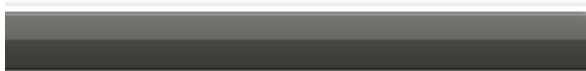
1.5.1.3 Delete User

- To delete a user, click on  and answer 'OK' on the popup.

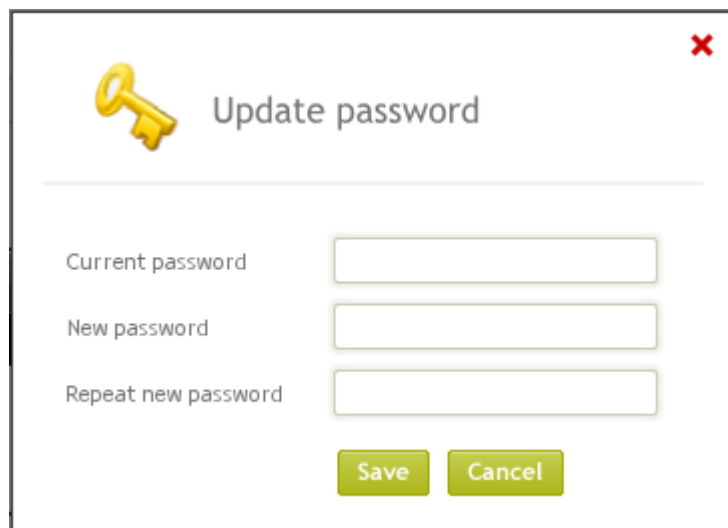
1.5.1.4 Changing password as user

When logged in to the LogServer you will see your username and a logout button in the right corner.

Logged in as: [admin](#) | [Log out](#)
Rows in database: 11783 Date: 2009-03-02 15:50 Version: 3.4.0



Pressing the username will popup a "Update password" dialogue.



The dialog box is titled "Update password" and features a yellow key icon. It contains three input fields: "Current password", "New password", and "Repeat new password". At the bottom, there are two buttons: "Save" and "Cancel". A red 'X' icon is in the top right corner of the dialog box.

- Enter your old password
- Type in your new password
- Verify new password by re-typing it

1.5.2 Group Management

As default all new created users can see all log messages. To have it the opposite way you should remove the group `all` from the filter `all`. Then you create groups for different level of users and set the permissions on the filters for the groups you created.

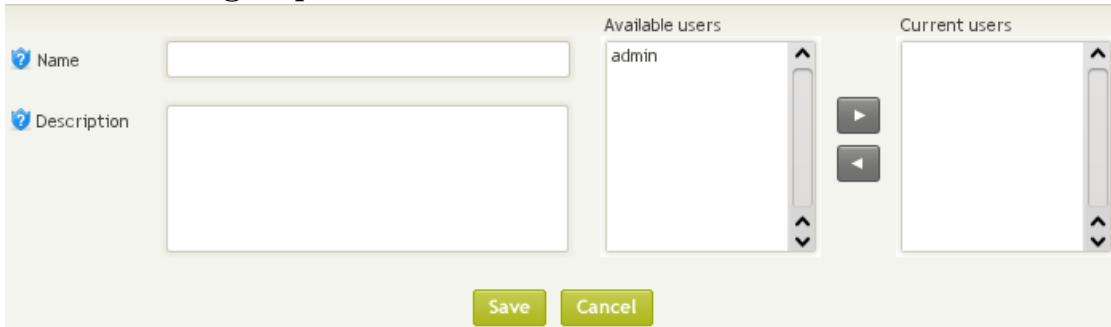
1.5.2.1 Default Groups

op5 LogServer comes with a couple of default groups that can't be deleted.


Group	Description
Filter administrators	Create/Manage Global filters Create/Manage Summary reports
Import administrators	Import old logs from archive into DB
Report administrators	Create/Manage Auto reports No access to Summary reports
Settings administrators	Access/Change Settings
User administrators	Create/Manage Users/Groups
Summary viewers	View Summary Reports

1.5.2.2 Add Group


To add a new group click on 



The screenshot shows a web-based form for adding a new group. On the left, there are two text input fields labeled 'Name' and 'Description'. To the right of these fields are two list boxes: 'Available users' (containing 'admin') and 'Current users' (empty). Between the list boxes are two arrow buttons for moving users. At the bottom of the form are 'Save' and 'Cancel' buttons.

- Fill in Name
- Description
- Select and move the users you will assign/remove to this group
- And press 

1.5.2.3 Edit Group

- To edit a group, click on  or doubleclick on the row of the group.

1.5.2.4 Delete Group

- To delete a group, click on  and answer 'OK' on the popup.

1.5.3 Audit tracking

Since version 3.5.0 of op5 LogServer we have included audit tracking to make sure an administrator can see what the users have been doing. The following actions are logged:

- Password and settings changes
- Logging in and out
- Creating, editing, deleting and viewing of auto reports
- Adding, editing, deleting and viewing users and groups
- Creating, editing, deleting and viewing of summary reports
- Changing filter permissions
- Importing logs
- Creating, editing and deleting filters
- Making filters global/private and viewing/chaning permissons on filters.
- Importing/exporting filters
- Exporting result sets to CSV.

Everthing is logged via syslog so the logs will show up in the GUI.

Two filters are added to make it easy to either see or hide the audit messages:

Filtername	Description
audit	Shows all audit messages - usefull for admins.
all except audit	Shows everything execept for audit messages. This is useful as a base for other filters, so that users don't see audit messages

Chapter 2

Configuring Clients

2.1 Windows Machines

To make a Windows computer send their logs to LogServer you have to download the Windows Syslog Agent from <http://www.op5.com/support> and install it.

Windows Syslog Agent sends the Windows Event Log content to the IP address of your op5 LogServer, and can optionally send plain text log files too – for applications that keep their own logs.

For detailed information on how to set up and use Windows Syslog Agent, please read op5 SyslogAgent User Manual available from <http://www.op5.com/support>

2.2 UNIX Machines

A UNIX machine has built-in support for syslog and hence you do not need to install any extra software.

2.2.1 syslogd

On most systems, you will find a config file called `/etc/syslog.conf` – this is where you enter the host name or IP address of your op5 LogServer host.

If your op5 LogServer host is on IP address 172.16.32.64, and you want to forward all facilities to it, append the following to `/etc/syslog.conf` and restart your syslog daemon:

```
*.* @172.16.32.64
```

some systems do not understand `*.*` – if this is the case you have to enter all facilities separately.

```
auth.* @172.16.32.64
authpriv.* @172.16.32.64
cron.* @172.16.32.64
daemon.* @172.16.32.64
ftp.* @172.16.32.64
kern.* @172.16.32.64
lpr.* @172.16.32.64
mail.* @172.16.32.64
mark.* @172.16.32.64
news.* @172.16.32.64
security.* @172.16.32.64
syslog.* @172.16.32.64
user.* @172.16.32.64
uucp.* @172.16.32.64
local0.* @172.16.32.64
local1.* @172.16.32.64
local2.* @172.16.32.64
local3.* @172.16.32.64
local4.* @172.16.32.64
```

```
local5.*    @172.16.32.64
local6.*    @172.16.32.64
local7.*    @172.16.32.64
```

Note that on some system, notably Solaris, the blank between the facility and the receiving host has to be made up of tabs, not spaces.

For details on how to configure syslog.conf, do a

```
man syslog.conf
```

on the machine you are configuring.

2.2.2 syslog-ng

More and more clients uses syslog-ng for sending syslog messages to a loghost.

If you use syslog-ng you can benefit from the stability to use tcp connection instead of the standard udp.

Sample /etc/syslog-ng/syslog-ng.conf to setup logging to loghost.

```
# all known message sources
source s_all {
    # message generated by Syslog-NG
    internal();
    # standard Linux log source (this is the default place for the syslog())
    # function to send logs to)
    unix-stream("/dev/log");
    # messages from the kernel
    file("/proc/kmsg" log_prefix("kernel: "));
};

destination d_loghost {
    tcp("172.16.32.64" port(514));
};

# send everything to loghost
log {
    source(s_all);
    destination(d_loghost);
};
```

2.2.3 Sending Text Files to LogServer

Some applications do not send their logs to syslog, but store them in a file on disk.

Most applications can be configured to use syslog, and changing the configuration of those applications should be your first hand choice.

Another option is using tail and logger to read the log file, and send appended lines to syslog. This command will read /var/log/myapp.log and send it to syslog as facility daemon and severity info.

```
tail -f /var/log/myapp.log | logger -p daemon.info
```

You can use a command like the one above for your application, and make sure it is executed on reboot – on many systems this can be done by placing the command in /etc/rc.local

2.3 Other Equipment

Many devices – from broadband firewalls for the home to office printers – can send their log files to a syslog server.

Look at the manual for your respective devices for information on how to fill out the syslog server.

Chapter 3

op5 LogServer Technology

3.1 The Syslog Protocol and Implementations

Syslog was originally written by Eric Allman as part of his application sendmail¹ but turned out to be so useful that it was turned into a project of it's own in the 1980:s.

Syslog is not only a protocol, but it also refers to various syslog implementations such as the local syslog daemon that takes care of local logging on any UNIX computer.

In 2001, RFC 3164² was published as an effort to unify syslog implementations.

3.1.1 Usage

On UNIX, most applications send their logs to the syslog process running on the same machine. This process then either stores the messages locally – in /var/log – or sends them to a syslog server for central storage.

All logging machines send their log data using TCP/IP to port 514

¹sendmail was the de-facto standard email server for two decades.

²Available at <http://tools.ietf.org/html/rfc3164>

on the receiving log server. Typically syslog uses UDP, but modern implementations such as op5 LogServer also support TCP. Most log servers simply store this data in text files, and retrieving historical data is a manual procedure and often impossible – unlike op5 LogServer where you have an easy-to-use graphical interface with easy import from archives.

3.2 op5 LogServer components

Syslog-ng

Syslog-ng is the component that receives and stores syslog data.

If you want to know more about syslog-ng, look at <http://www.balabit.com/network-security/syslog-ng/>

PostgreSQL

Since op5 LogServer 3.0 all data is stored in a PostgreSQL database for a limited amount of time, for easy access from the web interface.

Apache Web Server with PHP

The web interface is written in PHP and served by an apache web server.

3.3 LogServer Storage

LogServer has three storage facilities. Data is written to all three of these upon being received – however it is deleted according to separate settings.

3.3.1 The PostgreSQL database

All messages are initially stored in the PostgreSQL database. This is used as the default source of information for the web interface.

The data in the PostgreSQL database is deleted after a configured amount of time. See chapter [1.4.0.3](#) on page [29](#) for more information.

3.3.2 Local Storage

Data is also bziped and saved to disk, for future reference as archived data. When you restore archived data, it is fetched from the local storage if it is possible, otherwise it is fetched from the remote storage.

The data in the local storage is deleted after a configured amount of time. See chapter [1.4.0.4](#) on page [30](#) for more information.

3.3.3 Remote Storage

The remote storage has the same information as the local storage, but it is meant for saving data over a longer period of time.

Normally, this is located on a file server, where it is also backed up.

The data in the remote storage is deleted after a configured amount of time – see chapter [1.4.0.5](#) on page [31](#) for more information.

Appendix A

Installation

A.1 Basic Installation

If you have bought an op5 hardware appliance, you should install op5 System on it.

Installation of op5 System, any op5 Hardware and basic configuration of the system, such as IP address and SMTP relay server, is covered in op5 Installation and Configuration Customer Guide where you also find a list of recommended helper utilities for your administrators desktop.

If you have not received op5 Installation and Configuration Customer Guide, please notify [op5 Support](#).

A.2 Installing LogServer

LogServer is delivered as tar.gz files to be installed onto op5 System, or the official CentOS or RedHat Enterprise Linux 5. See www.op5.com/support/ for hardware requirements.

If you install it on op5 System and have a support agreement, the support includes not only LogServer but also op5 System. If you use another vendor for your operating system, please contact their support.

A.2.1 Obtaining tar.gz files

Download the tar.gz files from our Support Website, <http://www.op5.com/support> using your user name and password.

If you have not received a user name and password, please notify op5 Support.

When you have downloaded the files; copy them onto your op5 server root directory (/root)¹, then run the command

```
cd /root
tar xvzf op5-logserver*.tar.gz
cd logserver*
./install.sh
```

This will install LogServer. Then you can point your web browser to the machine and log on to your newly installed op5 LogServer. . .

A.3 Updating

If you run your LogServer on op5 System, you can update all installed packages by logging on to your server via SSH and then type:

```
yum update2
```

For alternative ways of updating, such as offline updates or other, please contact op5 Support³ or look at the op5 System documentation.

¹If you use Macintosh or UNIX, you can copy files to your server using scp. If you use Windows, you can use WinSCP.

²you can't update from 2.x to 3.x with yum update, but once 3.x is installed you can update your system.

³op5 Support can be reached at support@op5.com or at +46-31-7740924

A.4 Upgrading

Attention If you are going to upgrade from op5 LogServer 2.x you have to do it in the following steps:

- upgrade to op5 LogServer 3.0
- then upgrade to op5 LogServer 3.5.0

When migrating from op5 LogServer 2.x there will be a migration process during installation/updating.

The following will be migrated by default:

- Users/Passwords
- Settings for Archive⁴
- Filters

To Upgrade your system from a 2.x release you follow the steps on [A.2.1 Obtaining tar.gz files](#), and follow the on-screen instructions.

During the last step on the upgrade the installation asks if you want to convert your archive to the new format, this will take a lot of time if you have a large archive.

You can always start the convert process after the installation is done by executing

```
/opt/logserver/migrate2to3/convert.sh <src_dir> <dest_dir>
```

<src_dir> - your old 2.x logs are.

<dest_dir> - the local or remote archive location.

```
Do you want to convert all logs (Note: will take a lot of time, default is YES)
[Yes/No] ?
yes
Enter temporary directory path for migration of old log data (it must have enough space, default is /tmp/logserver-migrate)
[/tmp/logserver-migrate]?

Migrate logs from [/opt/logserver/local]
[Yes/No] ?

Remote directory points to the same place as local.
Converting...
Migration process is completed!
```

⁴Keep in remote storage Forever will be converted to 999 months.

Appendix B

Using Remote Storage

When you use remote storage, you have to create a folder and use it as a mount point by defining it in the file `/etc/fstab`:

<code>LABEL=/</code>	<code>/</code>	<code>ext3</code>	<code>data=writeback,noatime</code>	<code>1 1</code>
<code>LABEL=/boot</code>	<code>/boot</code>	<code>ext3</code>	<code>data=writeback,noatime</code>	<code>1 2</code>
<code>devpts</code>	<code>/dev/pts</code>	<code>devpts</code>	<code>gid=5,mode=620</code>	<code>0 0</code>
<code>tmpfs</code>	<code>/dev/shm</code>	<code>tmpfs</code>	<code>defaults</code>	<code>0 0</code>
<code>proc</code>	<code>/proc</code>	<code>proc</code>	<code>defaults</code>	<code>0 0</code>
<code>sysfs</code>	<code>/sys</code>	<code>sysfs</code>	<code>defaults</code>	<code>0 0</code>
<code>tmpfs</code>	<code>/tmp</code>	<code>tmpfs</code>	<code>nodev,nosuid,noatime</code>	<code>0 0</code>
<code>LABEL=SWAP-sda5</code>	<code>swap</code>	<code>swap</code>	<code>defaults</code>	<code>0 0</code>

Normally, everything in `/etc/fstab` is mounted on system startup. If you want to mount everything after editing, you can issue the command

```
mount -a
```

and if you want to check what is currently mounted, you can issue the command:

```
df
```

and mount and unmount using the commands `mount` and `umount`

B.1 Mounting a Windows Fileserver

Add a line to `/etc/fstab` where the first column, the device, is the Windows path for the share you want to mount, using forward slashes instead of backslashes.

The second column should be a path that exists where you want to mount it. If you would like to mount it on `/var/remotearchive` you can create the folder by issuing the command

```
mkdir -p /var/remotearchive
```

The third column should say `cifs` and the fourth, fifth and sixth should be defaults, 0 and 0 respectively.

```
//192.168.0.3/logs /opt/logserver/remote cifs defaults 0 0
```

B.2 Mounting an NFS share

If you have a UNIX environment, it is quite common to have NFS shares published from the file server using `/etc/exports` and then mounted on one or several client systems.

This chapter only describes NFS since it is the most common file server system, but if you are using a more advanced file server system – such as AFS or Coda – you can mount these just as on any other Linux system.

Add a line to `/etc/fstab` where the first column is the NFS server followed by a `:` and the path on the file server.

Let the second column be an existing path where you want the NFS share to be mounted – for this example `/var/remotearchive`

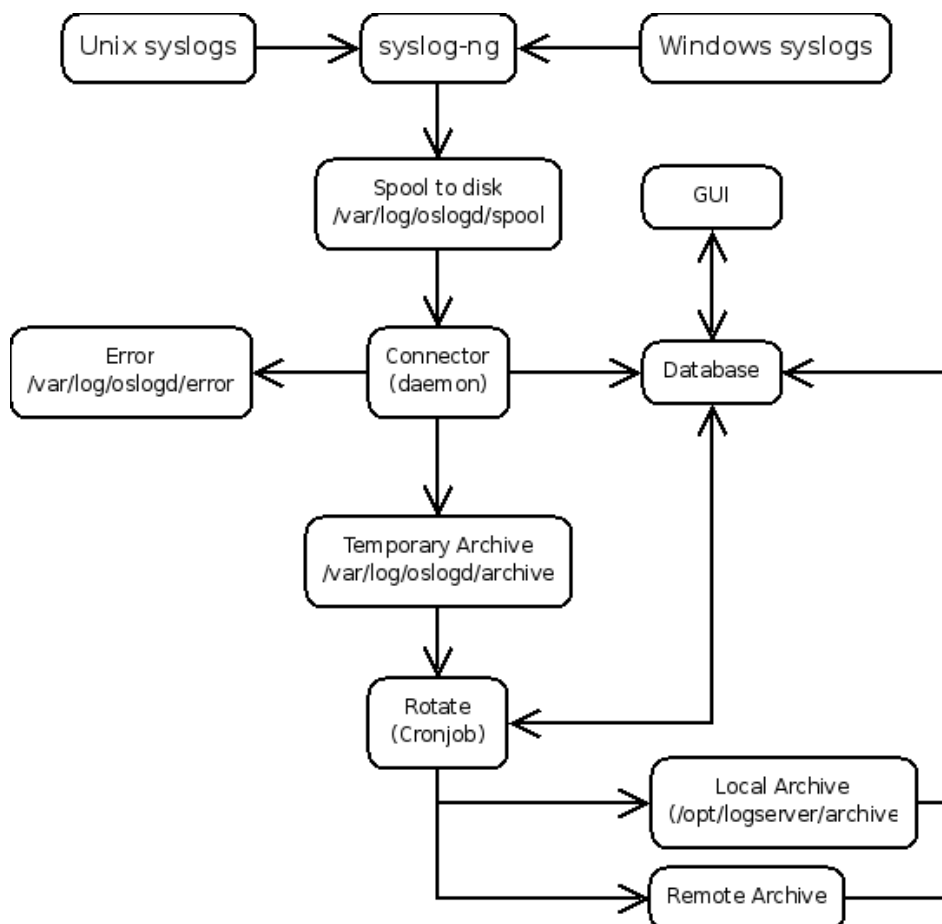
Let the third column be `nodev,nosuid` and the forth and fifth columns both be 0.

```
//192.168.0.3/exports/logs /opt/logserver/remote nfs nodev,nosuid 0 0
```

Appendix C

Workflow

Workflow of op5 LogServer.



C.1 Connector

- It's a Daemon (op5logserver-loader)
 - Runs two times/minute
1. Read logs from spool directory (/var/log/oslogd/spool)
 2. If they contain illegal chars, move to Error (/var/log/oslogd/error) and stop.
 3. Move logs to temporary archive (/var/log/oslogd/archive) and
 4. Insert logs to database

C.2 Rotate

- It's a cronjob
1. Runs every hour at xx.30 and put logs from temporary archive to local and remote archives
 2. Runs every hour checks database and local archive for old logs and rotate (configured in settings menu)
 3. Runs every day, checks remote archive for old logs and rotate (configured in settings menu)

Appendix D

Advanced DB Management

Original postgresql.conf file is tuned to run on low RAM machines (<3Gb RAM)

If you have a server with more than 3GB of RAM you should change the postgresql configuration to a file with larger memory settings.

- Stop PostgreSQL Service
- replace /var/lib/pgsql/data/postgresql.conf
- with /opt/logserver/postgresql-config/postgresql.conf
- Start PostgreSQL Service