



# OTUS SIEM

# OTUS SIEM

© 2014 [www.bitsteer.com](http://www.bitsteer.com)

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

# Table of Contents

<b>Part I Introduction</b>	<b>5</b>
1 System Requirements .....	6
2 How to Login to OTUS SIEM Online .....	7
3 Creating your OTUS account .....	12
<b>Part II The Raw Logs Search</b>	<b>15</b>
1 Raw Logs Search in detail .....	16
Instant Graph .....	20
Filtering data using filters .....	22
Notifications in detail .....	27
<b>Part III Data Handling</b>	<b>31</b>
1 Viewing and Downloading raw data .....	32
<b>Part IV Indexing log search</b>	<b>35</b>
<b>Part V Alerting</b>	<b>37</b>
1 Creating and Managing Alert Queries .....	38
2 Creating and Managing Alert Rules .....	43
Creating and Managing Alert Rules > Creating and Managing Rule Instances .....	48
3 Alerting > Viewing Alert Events .....	51
<b>Part VI Reporting</b>	<b>55</b>
1 Creating a report .....	61
2 Customizing a Report .....	66
<b>Part VII Configuration</b>	<b>69</b>
1 Creating and Managing Servers .....	70
2 Creating and Managing Groups & Distributions .....	73
3 Creating and Managing Distribution .....	75
Pull Distribution .....	76
SYSLOG Distribution .....	79
SNMP Distribution .....	83
<b>Part VIII Managing Settings</b>	<b>87</b>
<b>Part IX Creating and Managing Storage</b>	<b>91</b>
1 Creating and Managing Storage Rules .....	94

<b>Part X</b>	<b>User and Role Management</b>	<b>99</b>
1	Creating and Managing Users .....	100
2	Creating and Managing Roles .....	102
<b>Part XI</b>	<b>System</b>	<b>109</b>
1	System > Viewing system status .....	110
2	System > Viewing system events .....	111
<b>Part XII</b>	<b>Logged in User Settings</b>	<b>115</b>
<b>Part XIII</b>	<b>List of OTUS time formats</b>	<b>119</b>
	<b>Index</b>	<b>121</b>

**Part**



**Introduction**

# 1 Introduction

Hi and welcome to **OTUS, SIEM**.

**OTUS** is a management system for storing server, application, and network information on a centralized location. **OTUS SIEM** offers a fast and organized way to access, analyze, and act on your network data. Data analysis, intruder detection, and custom reports are some of the many features that are available. These functions are explained in more detail under their respective topics.

We at **OTUS** hope that your experience with our web application is a smooth, elegant and an enjoyable one. We have taken great efforts to put together this Help file so that you may refer to it in case of difficulty or troubleshooting.

If you still have questions or feedback to provide please contact support at: << place holder for e-mail address or contact numbers >>

## 1.1 System Requirements

This topic discusses the system requirements to run and use the application.

To run **OTUS, SIEM** successfully on your system you need to have these minimum requirements on your server and on your client side you must have a good Internet browser. On the back-end you need linux.

### Hardware

Small installation ( up to 50 servers )

<b>CPU:</b>	Minimum - 1 Pentium Processor or later for desktops or Xeon Dual core for Servers/Workstations.  Recommended - Pentium i Core (desktops/laptops) or Xeon Quad Core or above for Servers and Workstations
<b>Memory:</b>	2 GB
<b>Available disk space:</b>	80 GB

Medium Installation ( up to 100 servers )

<b>CPU:</b>	Minimum - 2 Pentium Processor or later for desktops or 2 Xeon Dual core for Servers/Workstations.  Recommended - 2 Pentium i Core (desktops/laptops) or Xeon Quad Core or above for Servers and Workstations
<b>Memory:</b>	4 GB

<b>Available disk space:</b>	160 GB
------------------------------	--------

Large Installation ( up to 200 servers )

<b>CPU:</b>	Minimum - 8 Pentium Processor or later for desktops or 4 Xeon Dual core for Servers/Workstations.  Recommended - 8 Pentium i Core (desktops/laptops) or 4 Xeon Quad Core or above for Servers and Workstations
<b>Memory:</b>	8 GB
<b>Available disk space:</b>	320 GB

For Very large installation ( 200+ servers)  
contact [hello@bitsteer.com](mailto:hello@bitsteer.com)

#### Ports

<b>Open Ports:</b>	80 (HTTP) , 443( HTTPS) , 514 (SYSLOG) , 161 ( SNMP), 162 ( SNMP TRAP)
<b>Clustering Ports for very large installations:</b>	9200 - 9300 ElasticSearch 9369, 35197 RabbitMQ 5432 PostgreSQL

#### Software and Other Requirements

The software requirements are:

<b>Operating System:</b>	Windows 2000, Windows NT 4.0, (Service Pack 6a or later and IE 6.0+), Windows XP Professional, Windows 2003 Server, Windows Vista (All), Windows 7, Windows 8
<b>Internet Browser</b>	Firefox 3.0 or later version (recommended) Google Chrome (recommended) Internet Explorer 9.0 or later version Safari or Opera (latest versions)

## 1.2 How to Login to OTUS SIEM Online

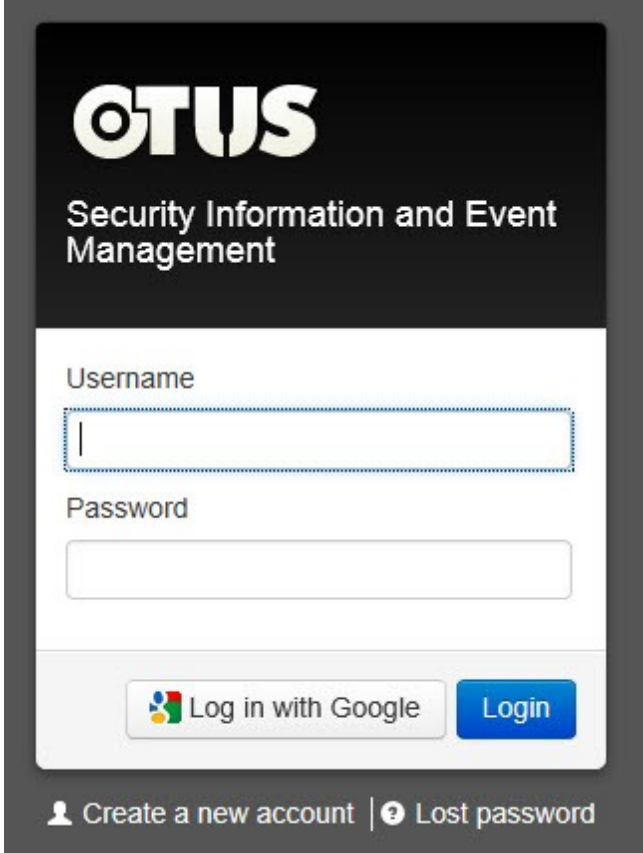
This topic explains how to login to the **OTUS SIEM** online application. You may use the Username and password provided to you (when you purchased the product) to login. Alternatively you could also login using your Google account. Both login procedures are explained in this topic. How to logout from the application is also explained.

**Note:** If you do not have an **OTUS** account you could register for one. Please refer the [Creating your OTUS account](#) topic for details.

### To login to OTUS using Username and Password

1. Open your web browser (Internet Explorer, Firefox, Google Chrome or Safari) and enter the URL of your **OTUS SIEM** login page in your URL field and click **Enter**.

On successful loading of your page you must see the following login fields.



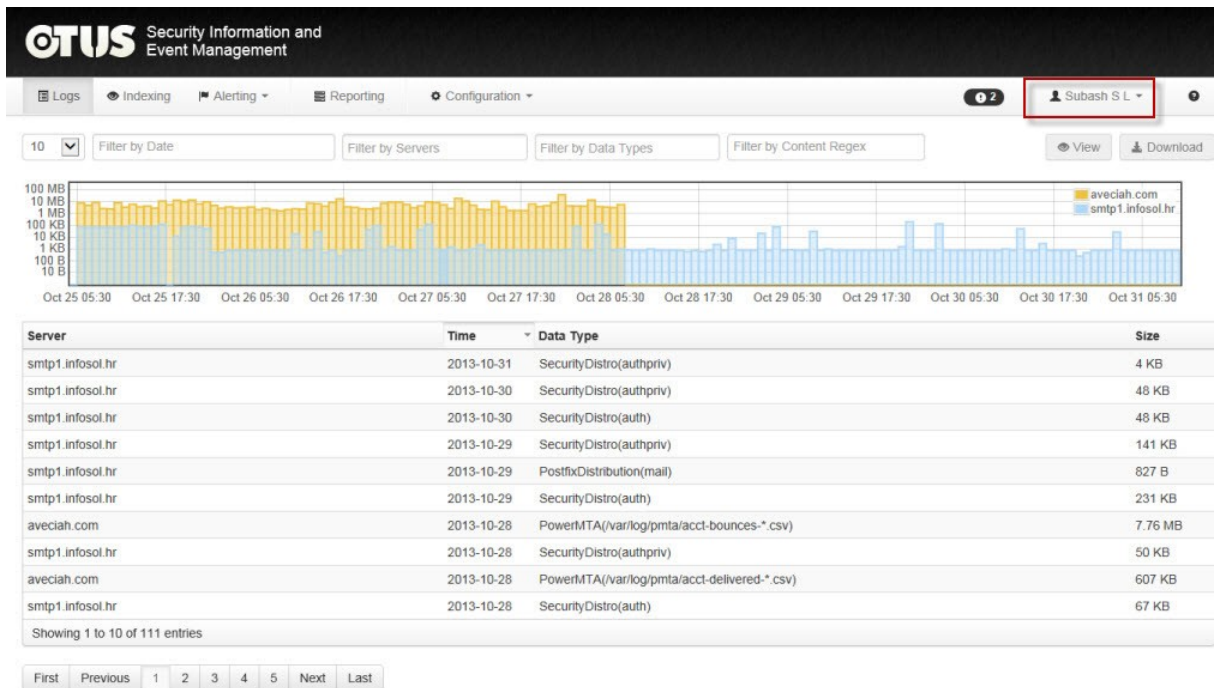
The screenshot shows the OTUS SIEM login interface. At the top, the OTUS logo is displayed in white on a black background, followed by the text 'Security Information and Event Management'. Below this is a white login form. The form contains two input fields: 'Username' and 'Password'. The 'Username' field is currently empty and has a dotted border. Below the 'Password' field are two buttons: 'Log in with Google' and 'Login'. At the bottom of the form are two links: 'Create a new account' and 'Lost password'.

2. Enter your Username in the **Username** field.
3. Enter your password in the **Password** field.

**Note:** If you have forgotten your password click the **Lost password** link. How to recover your password is explained under the section **To recover lost password**, below.

4. Click **Login**. On successful login the home page of the application opens.



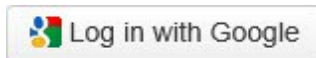


**Note:** Notice your username (encircled in bold) on the top right of the image.

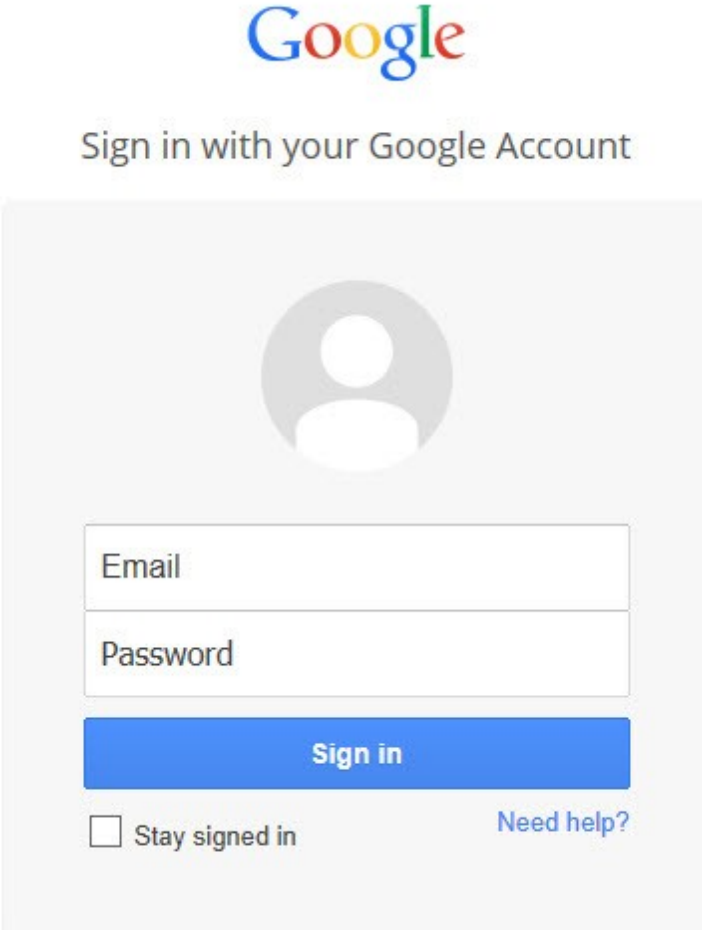
### To login to OTUS using your Google account

1. Access the home page as mentioned in **Step 1** of the previous section.

2. Click the **Log in with Google**



button. The web page refreshes to display the following fields.

The image shows the Google sign-in interface. At the top is the Google logo in its multi-colored font. Below it is the text "Sign in with your Google Account". The main content is a light gray rounded rectangle containing a circular profile picture placeholder. Below the placeholder are two input fields: "Email" and "Password". Under the "Password" field is a blue "Sign in" button. At the bottom left of the form is a checkbox labeled "Stay signed in", and at the bottom right is a blue link labeled "Need help?".

Google

Sign in with your Google Account

Email

Password

Sign in

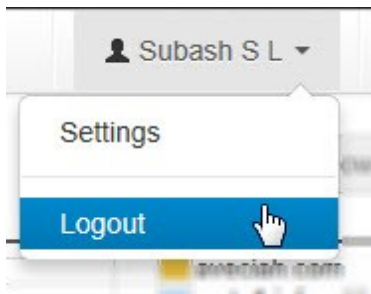
Stay signed in [Need help?](#)

3. Enter your gmail id (one that you use to access your Google account) in the **Email** field.
4. Enter the password for the email (Google account) in the **Password** field.
5. Click **Sign in**. If the login credentials are correct the home page (image displayed above) of the application is displayed.

**Note:** Access to **OTUS** is based on the role a user is assigned. For example the **always** role permits a user to access the application anytime. The **working\_hours** role permits a user to access the application only during the time defined for the **working\_hours** role which may be from 09:00 AM to 05:00 PM.

#### To logout of OTUS

1. Click on the username located on the top right of the home page. The following menu is displayed.



2. Click **Logout**.

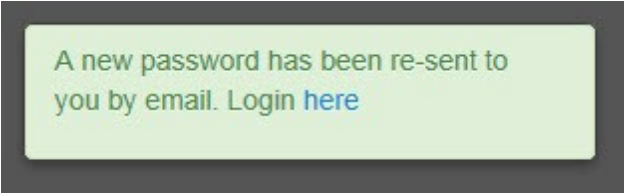
**Note:** Before leaving the application please ensure that you do not have any unsaved data left open or unsaved data that you were changing.

### To recover lost password

1. From the login page that displays the fields for Username and Password click the **Lost Password** link. The webpage refreshes to display the following fields.

A screenshot of the OTUS password recovery form. The top section has a black background with the OTUS logo in white, followed by the text 'Security Information and Event Management'. Below this is a white form area with an 'Email' label and a text input field. At the bottom of the form, there are two buttons: a grey button with a left arrow and the text 'Go back to Login', and a blue button with the text 'Recover'.

2. Enter your email in the **Email** field. This is the email that you used when you registered for your **OTUS** account.
3. Click **Recover**. A message indicating that your new password is sent to your email is displayed.



A new password has been re-sent to you by email. [Login here](#)

4. Open your email to use the reset password.


## 1.3 Creating your OTUS account

If you do not have an account or if you do not have a Google account you can also register for one, online. This topic explains how.

### To register on OTUS and obtain an account

1. Open your web browser (Internet Explorer, Firefox, Google Chrome or Safari) and enter the following URL in your URL field and click **Enter**.


On successful loading of your page you must see the following login fields.




**OTUS**  
Security Information and  
Event Management

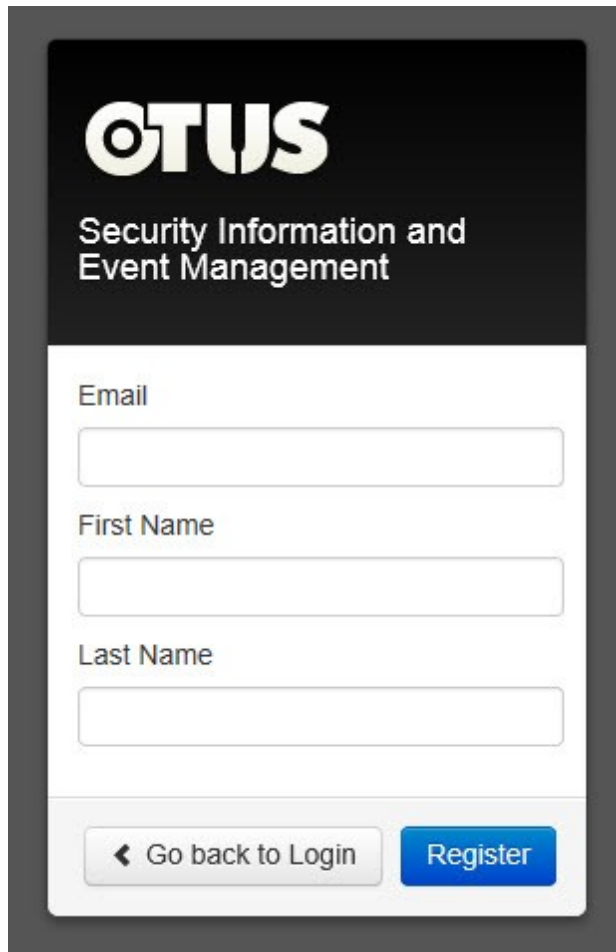
Username

Password

 Log in with Google

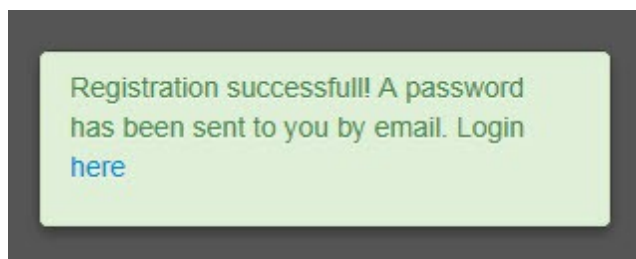
 [Create a new account](#)

2. Click the **Create a new account** link. The web page refreshes to display the following fields.



The screenshot shows a registration form for OTUS. At the top, the OTUS logo is displayed in white on a black background, followed by the text "Security Information and Event Management". Below this, there are three input fields: "Email", "First Name", and "Last Name". At the bottom of the form, there are two buttons: a grey button with a left-pointing arrow and the text "Go back to Login", and a blue button with the text "Register".

3. Enter a valid email id in the Email field.
4. Enter your first name in the **First Name** field.
5. Enter your last name in the **Last Name** field.
6. Click **Register**. A successful registration message is sent to the email that was used for registration.

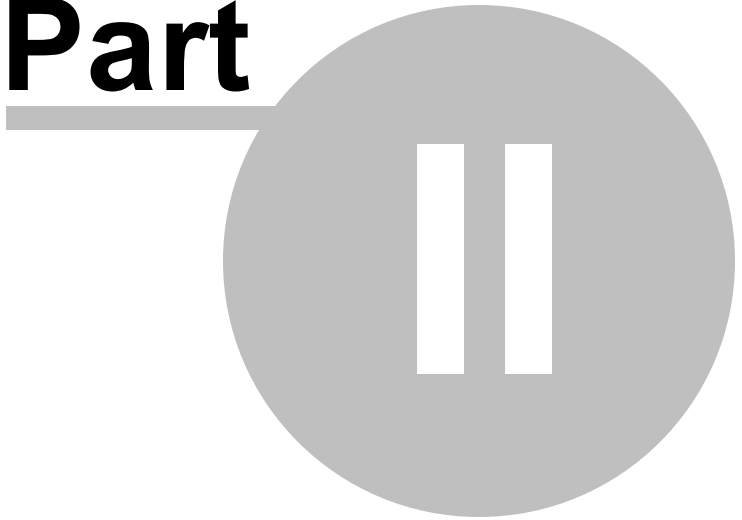


**Note:** To go back to the login page click

◀ Go back to Login



# Part



**The Raw Logs  
Search**

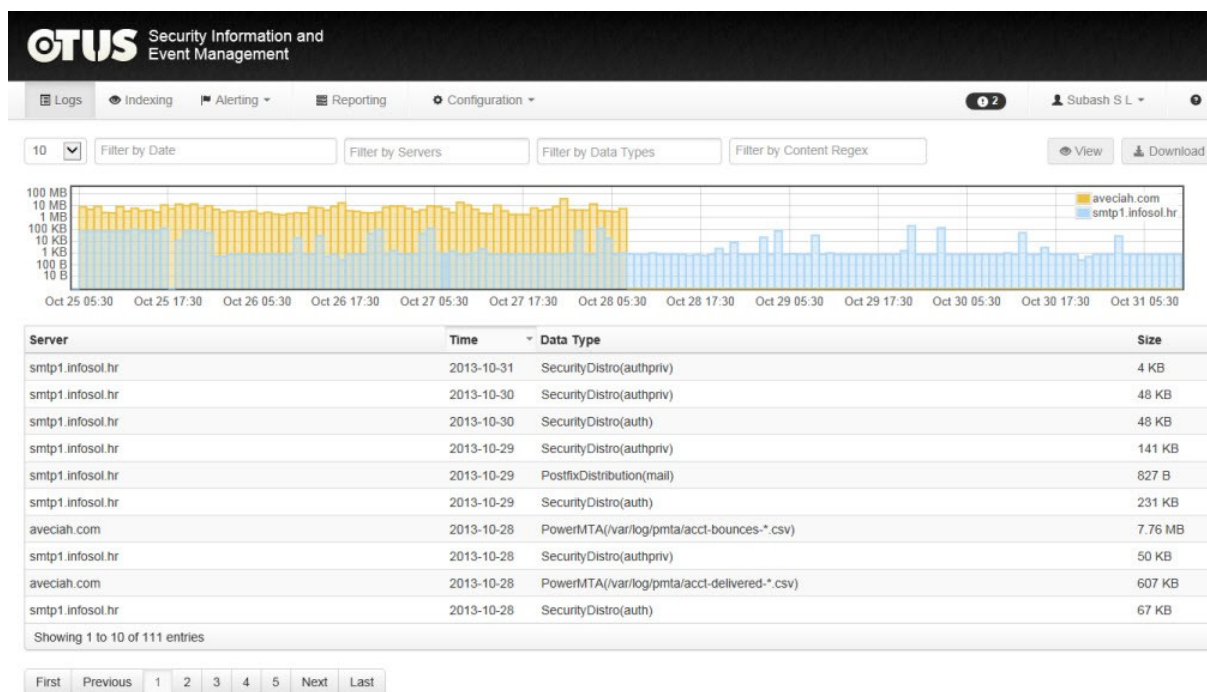
## 2 The Raw Logs Search

The Raw Logs Search page is your starting point from where you can access the various functionality of the **OTUS SIEM** online application. The various modules for the various functionality can be accessed via the various menus. The home page and how to navigate the menus are explained in this chapter.

### 2.1 Raw Logs Search in detail

This topic discusses the Raw Logs Search in detail. The **Home Page** is the page that is displayed immediately after a successful login.

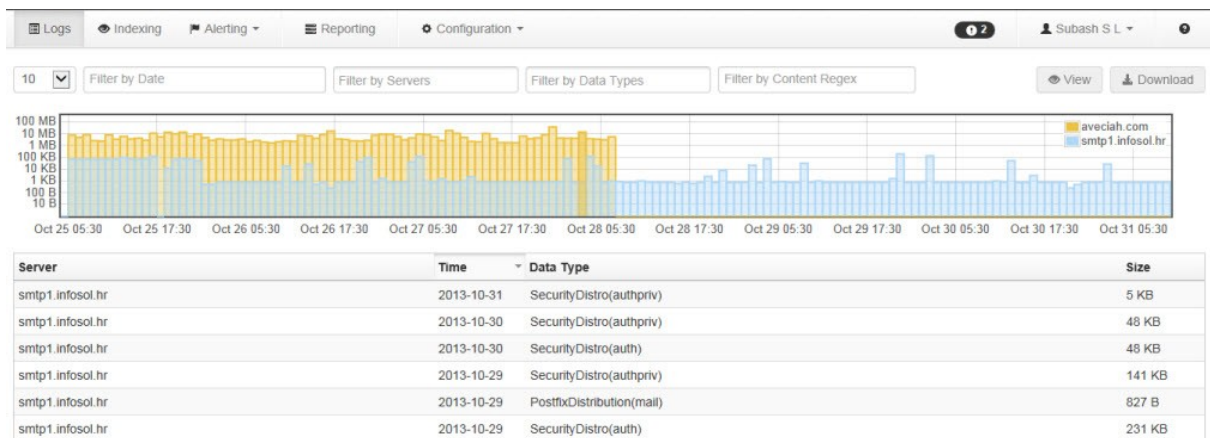
Raw log files are files that are not indexed. They are displayed here in their original format as they come into the system. All data is stored in raw log file format. Data that is indexed is also stored in indexed or tabular form, but the raw log file format remains.



#### The Main Log area

By default when you login for the first time the details under the **Logs** are displayed as shown below. By default 10 entries are displayed per page but this can be changed.

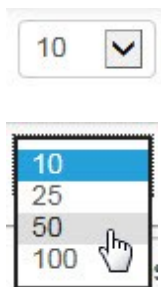




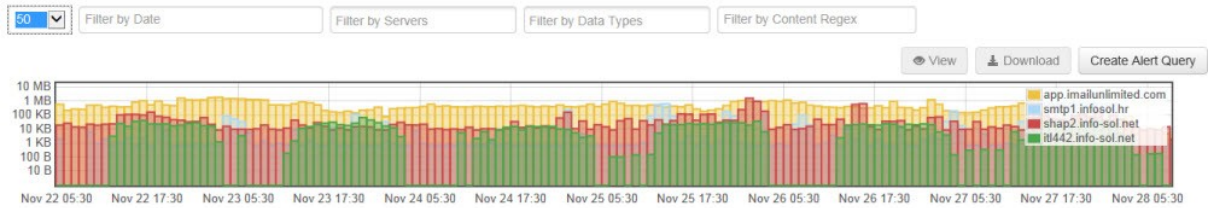
Additional pages of information can be accessed via the page numbers below the screen.



Another option would be to select more number of detail lines per page and this can be done by clicking an option from the **No. of lines per page** filter as shown below.



In the above case, the page would instantly refresh to display 50 lines of details per page as shown in the image below.



Server	Time	Data Type	Size
shap2.info-sol.net	2013-11-28	NginxDistro(/var/log/nginx/apps.info-sol.net-access.log*)	82 B
shap2.info-sol.net	2013-11-28	NginxDistro(/var/log/nginx/demo.otus-logging.com-access.log*)	9 KB
app.imailunlimited.com	2013-11-28	SecurityDistro(kern)	35 KB
shap2.info-sol.net	2013-11-28	SecurityDistro(authpriv)	24 KB
app.imailunlimited.com	2013-11-28	SecurityDistro(authpriv)	119 KB
smtp1.infosol.hr	2013-11-28	SecurityDistro(auth)	841 B
itl442.info-sol.net	2013-11-28	NginxDistro(/var/log/nginx/brojac.itlab.hr-access.log*)	364 B
shap2.info-sol.net	2013-11-28	SecurityDistro(auth)	12 KB
shap2.info-sol.net	2013-11-28	PostfixDistribution(mail)	9 KB
smtp1.infosol.hr	2013-11-28	SecurityDistro(authpriv)	4 KB
app.imailunlimited.com	2013-11-27	NginxDistro(/var/log/nginx/mailtools.imailtools.com-access.log*)	79 KB
itl442.info-sol.net	2013-11-27	NginxDistro(/var/log/nginx/brojac.itlab.hr-access.log*)	300 KB
shap2.info-sol.net	2013-11-27	NginxDistro(/var/log/nginx/pin.info-sol.net-access.log*)	10 KB
shap2.info-sol.net	2013-11-27	NginxDistro(/var/log/nginx/trac.info-sol.net-access.log*)	91 KB
shap2.info-sol.net	2013-11-27	NginxDistro(/var/log/nginx/provserver.info-sol.net-access.log*)	17 KB
smtp1.infosol.hr	2013-11-27	SecurityDistro(authpriv)	2.39 MB
smtp1.infosol.hr	2013-11-27	SecurityDistro(auth)	5.25 MB
app.imailunlimited.com	2013-11-27	NginxDistro(/var/log/nginx/app.imailunlimited.com-access.log*)	4.49 MB
smtp1.infosol.hr	2013-11-27	PostfixDistribution(mail)	822 B
shap2.info-sol.net	2013-11-27	SecurityDistro(authpriv)	171 KB
shap2.info-sol.net	2013-11-27	PostfixDistribution(mail)	63 KB
shap2.info-sol.net	2013-11-27	NginxDistro(/var/log/nginx/demo.otus-logging.com-access.log*)	576 KB
app.imailunlimited.com	2013-11-27	SecurityDistro(authpriv)	5.04 MB
app.imailunlimited.com	2013-11-27	NginxDistro(/var/log/nginx/rbchecker.imailtools.com-access.log*)	10 KB
shap2.info-sol.net	2013-11-27	SecurityDistro(auth)	119 KB
app.imailunlimited.com	2013-11-27	SecurityDistro(kern)	144 KB
shap2.info-sol.net	2013-11-27	NginxDistro(/var/log/nginx/apps.info-sol.net-access.log*)	152 KB
smtp1.infosol.hr	2013-11-26	PostfixDistribution(mail)	3 KB
shap2.info-sol.net	2013-11-26	NginxDistro(/var/log/nginx/trac.info-sol.net-access.log*)	26 KB
shap2.info-sol.net	2013-11-26	SecurityDistro(authpriv)	678 KB
smtp1.infosol.hr	2013-11-26	SecurityDistro(authpriv)	193 KB
shap2.info-sol.net	2013-11-26	NginxDistro(/var/log/nginx/provserver.info-sol.net-access.log*)	15 KB
shap2.info-sol.net	2013-11-26	SecurityDistro(auth)	937 KB
app.imailunlimited.com	2013-11-26	SecurityDistro(authpriv)	1.01 MB
shap2.info-sol.net	2013-11-26	NginxDistro(/var/log/nginx/pin.info-sol.net-access.log*)	11 KB
shap2.info-sol.net	2013-11-26	NginxDistro(/var/log/nginx/demo.otus-logging.com-access.log*)	176 KB
smtp1.infosol.hr	2013-11-26	SecurityDistro(auth)	262 KB
app.imailunlimited.com	2013-11-26	SecurityDistro(kern)	145 KB
itl442.info-sol.net	2013-11-26	NginxDistro(/var/log/nginx/brojac.itlab.hr-access.log*)	270 KB
app.imailunlimited.com	2013-11-26	NginxDistro(/var/log/nginx/mailtools.imailtools.com-access.log*)	65 KB
shap2.info-sol.net	2013-11-26	PostfixDistribution(mail)	29 KB
app.imailunlimited.com	2013-11-26	NginxDistro(/var/log/nginx/rbchecker.imailtools.com-access.log*)	29 KB
app.imailunlimited.com	2013-11-26	NginxDistro(/var/log/nginx/app.imailunlimited.com-access.log*)	11.51 MB
shap2.info-sol.net	2013-11-26	NginxDistro(/var/log/nginx/apps.info-sol.net-access.log*)	322 B
shap2.info-sol.net	2013-11-25	NginxDistro(/var/log/nginx/provserver.info-sol.net-access.log*)	16 KB
app.imailunlimited.com	2013-11-25	NginxDistro(/var/log/nginx/app.imailunlimited.com-access.log*)	14.48 MB
shap2.info-sol.net	2013-11-25	SecurityDistro(authpriv)	1.07 MB
app.imailunlimited.com	2013-11-25	NginxDistro(/var/log/nginx/mailtools.imailtools.com-access.log*)	64 KB

Showing 1 to 50 of 1,307 entries

Basically what this page displays is the details of the raw log files and also provides means to search this data.

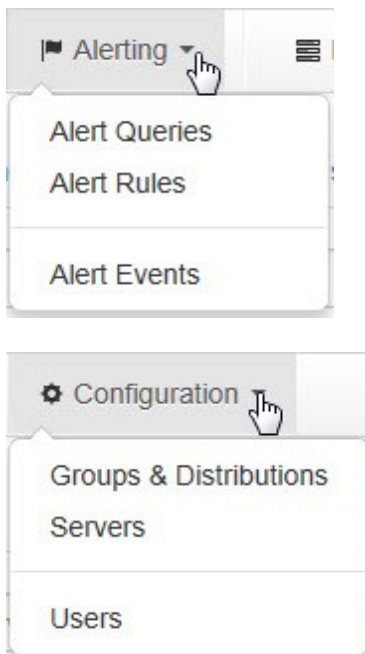
### The Instant Graph

This graph shows the raw file log size in that time range across various servers. It has several other functionality too. For more details click the [Instant Graph](#)<sup>[20]</sup> topic.

### Accessing the modules and menus

You can access the various modules by clicking the **Logs**, **Indexing** and **Reporting** links. Further options for filtering and categorization are provided once a particular function is accessed.

To access menus as in the case of the **Alerting** and **Configuration** menus, click the tile and a drop-down appears.



We have already seen the Username menu in the [How to Login to OTUS SIEM](#)<sup>[7]</sup> Online topic.

### Latest notifications button

This button is located very near the Username menu. Clicking on it displays the most recent notifications in a pop-up as shown below.



You can click a notification to reveal more details of the notification in a table-view format. You can also click **Show All** inside the pop-up to view all the notifications in the main log area or table-view format.

**Note:** Please view the topic [Notifications in detail](#)<sup>[27]</sup> for more information on notifications.

### Filtering the Data

You can also filter the data of the logs displayed on the **Main Log Area** by clicking one or more of the filters. Please view the [Filtering Data using filters](#)<sup>[22]</sup> topic for details.

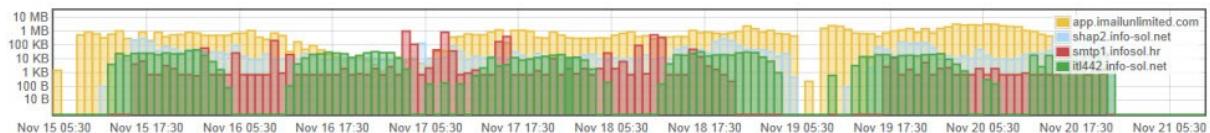
### Create Alert Query button



Clicking this button leads to creating raw alert query based on search parameters.

## 2.1.1 Instant Graph

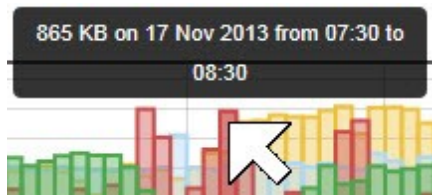
The instant graph shows you a snapshot of the raw file log transfer on the servers for the past two weeks beginning with the current date, located at the far right.



The higher the bars the greater is the transfer rate. A legend on the far right also indicates which colored bar represents the data transfer of server.

Other features of the graph are:

- Mousing over a bar in the graph pops up a call-out indicating the amount of log transfer on that particular date and the start-time and end-time of the transfer. The call-out also mentions the amount of data transferred on that date and for the particular time period.

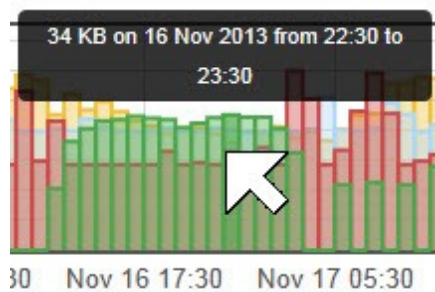


• Zooming in on the graph - this facilitates viewing more detailed information in a more detailed display of the graph. Zooming in is explained below.

### To zoom in on the graph (for information of transfer in Days)

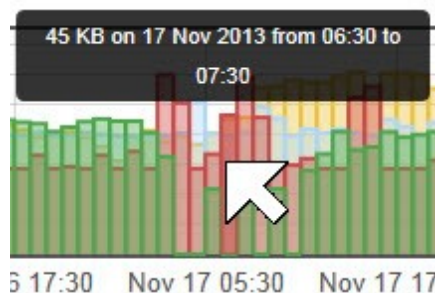
Use this functionality to determine the transfer of log for a particular number of days. (In our example from 23:30 hours, November 16, till 7:30 hours November 17)

1. Position the mouse over the graph such that the tool-tip (call-out) displays the information for the start day and time, i.e 11:30 PM, November 16.

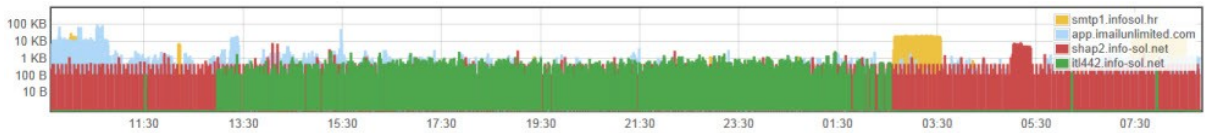


**Note:** Mouse cursor in the image above has been emphasized to show what it points accurately. Subsequent images may also show the mouse cursor in this emphasized form for clarity purposes.

2. Click and drag across the graph till the tool-tip displays the end day and time i.e 7:30 AM, November 17. You must see the following image.



3. Release the mouse button. The graph will redraw itself to display the corresponding information as displayed in the image below.

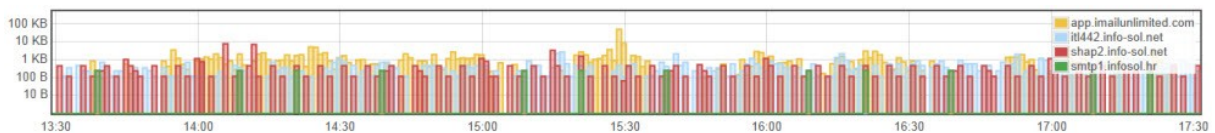


You can further drill down this image for finer details, such as information of transfer in hours and in minutes.

### To zoom in on the graph (for information of transfer in hours)

In our example we are going to find out finer details about the transfer between 13:30 and 17:30.

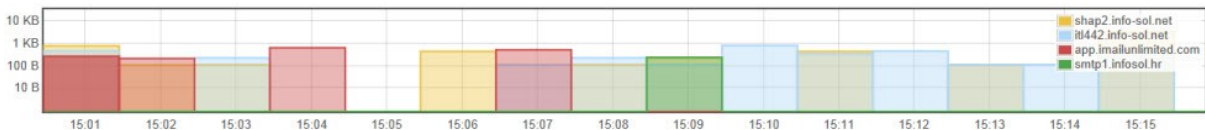
1. Position the mouse over the graph such that the tool-tip (call-out) displays the information for the start time, i.e 13:30 PM.
2. Click and drag across the graph till the tool-tip displays the end day and time i.e 17:30.
3. Release the mouse and the graph redraws itself to display an image as shown below.



### To zoom in on the graph (for information of transfer in Minutes)

In our example we are going to find out the details of the data transfer between 15:00 and 15:15.

1. Position the mouse over the graph till the tool-tip now displays the start time 15:00.
2. Click and drag across the graph till the tool-tip displays the end time i.e 15:30.
3. Release the and the graph redraws itself to display an image as shown below.



**Note:** Every time you zoom in, the table below the graph is also automatically updated. The **Filter By Date** field is automatically populated with the time and dates that you selected for zooming in.

## 2.1.2 Filtering data using filters

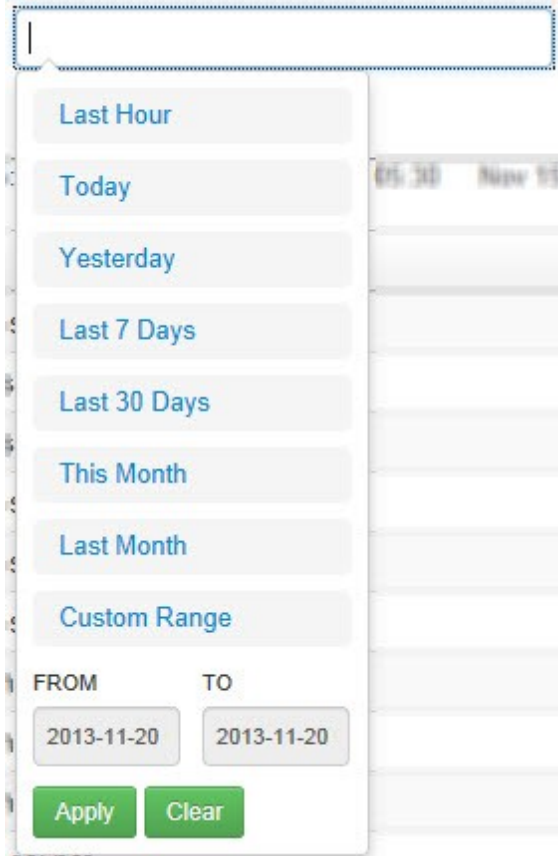
The data on the main log area can be filtered using one or more of several filters. This topic discusses using these filters.

**Note:** With one filter already in use you can add more filters to filter that data.

### To filter by Date

Filter by Date

1. Click inside the **Filter by Date** filter box. A drop-down of options is displayed.



2. Select an option (the first seven, **Last Hour** till **Last Month**) and the web page automatically refreshes to display the data for that selected filter.
3. Click the **Custom Range** option to set a **FROM** date and a **TO** date filter. In this case pop-up windows to select date appear as shown below.

The screenshot shows a date filtering interface. On the left, there is a vertical list of time-based filters: Last Hour, Today, Yesterday, Last 7 Days, Last 30 Days, This Month, and Last Month. Below these is a blue 'Custom Range' button with a mouse cursor pointing to it. Underneath the button are two input fields labeled 'FROM' and 'TO', both containing the date '2013-10-01'. At the bottom of this section are two green buttons: 'Apply' and 'Clear'. To the right of the filters are two calendar boxes for 'October 2013'. The left calendar has the 1st of October highlighted in blue. The right calendar has the 31st of October highlighted in blue. Above the calendars are two search boxes: 'Filter by Servers' and 'Filter by Data Types'.

4. Select a date from the calendar box on the left for the **FROM** date.
5. Select a date from the calendar box on the left for the **TO** date.
6. Click **Apply**. The web page refreshes to display the data applicable to the custom date filter.

**Note:** Click **Clear** to clear the filter and close the drop-down list.

#### To filter by server

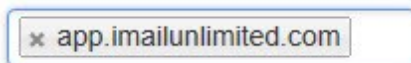
1. Click inside the **Filter by Servers** box. A drop-down of servers currently being tracked is displayed.



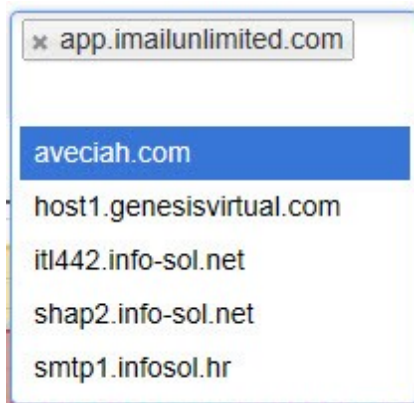


2. Select a filter from the list by clicking on it. The web page refreshes to display the logs and information pertaining to that server.

**Note:** You can select one or more servers using this filter. Let us assume the app.imailunlimited.com server is selected. Note that it shows up in the filter as follows.



To add one or more servers from the list of servers just click inside this filter again in the space adjacent to the already existing filter and the drop-down appears.

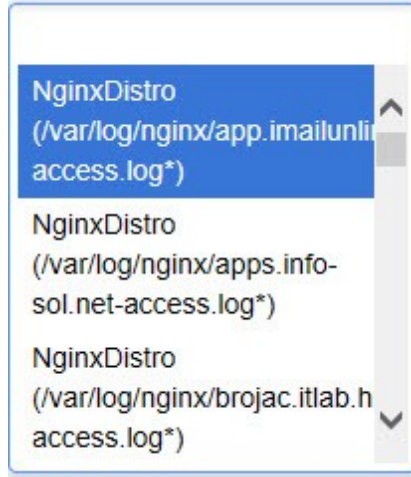


From here you can select another server. Repeat the steps to add servers. To remove a server from the filter click the "X" symbol of a server name from the filter. Also in the drop-down the cursor is seen blinking in the vacant space above the list of servers. If the list of servers is long and you would like to search (and subsequently select) a server just enter the name or the first few characters of the server's name in this space and the server you are searching for is located and listed in the drop-down list for you to select.

### To filter by Data Types

**Note:** A data type is the type of data that is stored. It consists of a distribution(path) for pull distributions or distribution(facility) for SYSLOG distributions.

1. Click inside the **Filter by Date Types** box. A drop-down of options is displayed.




2. Browse the list of data types from the drop-down and select one of your choice. The web page refreshes to display logs pertaining to that data type selected.

**Note:** As with the **Filter by Servers** filter, you can select multiple Data types in the **Filter by Data Types** filter also. Refer explanation in the previous section.

#### To filter using regular expressions (Regex)

1. Click inside the **Filter by Content Regex** box and enter a regular expression. For example to search for all linux related logs enter **linux** and press **Enter**. The web page refreshes to display logs related to the keyword "**linux**" or "**linux**" followed by any character or characters of any length without spaces. Other examples of regular expression include "**conn.\***"

(In our example the word "**conn.\***" is used in the filter which ideally means pages with "connect", or any record containing the characters "**conn**" followed by any character of any length without spaces, will

show in the results). From the list of log files displayed click  to view the contents of the log file by selecting the file (with your mouse). The following page is displayed.

Logfile content g\_mail/shap2.info-sol.net/PostfixDistribution/mail/2013/12/06.log

conn.\*

```
Dec 06 00:01:50 <mail.info> 10.10.10.110: shap postfix/smtpd[22356]: connect from localhost[127.0.0.1]
Dec 06 00:01:51 <mail.info> 10.10.10.110: shap postfix/smtpd[22356]: 0598C6D00E3: client-localhost[127.0.0.1]
Dec 06 00:01:51 <mail.info> 10.10.10.110: shap postfix/cleanup[22359]: 0598C6D00E3: message-id=<20131205230151.0598C6D00E3@shap.ztm.hr>
Dec 06 00:01:51 <mail.info> 10.10.10.110: shap postfix/smtpd[22356]: disconnect from localhost[127.0.0.1]
Dec 06 00:01:51 <mail.info> 10.10.10.110: shap postfix/qmgr[9794]: 0598C6D00E3: from=<logging-server@info-sol.net>, size=621, nrcpt=1 (queue active)
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/smtp[22360]: 0598C6D00E3: enabling PIX workarounds: disable_esmtp delay_dotcrif for ASPMX.L.GOOGLE.COM[173.194.78.27]:25
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/smtp[22360]: 0598C6D00E3: to=<notification@info-sol.net>, relay=ASPMX.L.GOOGLE.COM[173.194.78.27]:25, delay=1.6, delays=0.15/0.13/1.1/0.22, dsn=5.1.1, status=bounced (host ASPMX.L.GOOGLE.COM[173.194.78.27] said: 550-5.1.1 The email account that you tried to reach does not exist. Please try 550-5.1.1 do uble-checking the recipient's email address for typos or 550-5.1.1 unnecessary spaces. Learn more at 550 5.1.1 http://support.google.com/mail/bin/answer.py?answer=6596 wg1s1353850 67xjb.115 - gsmtpt (in reply to RCPT TO command))
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/cleanup[22359]: 9ED416D00E6: message-id=<20131205230152.9ED416D00E6@shap.ztm.hr>
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/bounce[22371]: 0598C6D00E3: sender non-delivery notification: 9ED416D00E6
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/qmgr[9794]: 9ED416D00E6: from=<>, size=3075, nrcpt=1 (queue active)
```

Follow

First Previous 1 2 3 4 5 Next Last 10

**Note:** Here additional filtering can be done in two ways. 1. Entering text inside the Search box (the one with the lens symbol inside) 2. Entering text in the Search box. 3. Creating one or more alerts. This is explained in the topic [Creating Alert Queries](#) <sup>38</sup>.

Entering a regex string such as "goog.\*" to say search for all instances of "Google" or "googlebot" in the search box returns results as shown below.

Logfile content g\_mail/shap2.info-sol.net/PostfixDistribution/mail/2013/12/06.log

goog.\*

```
Dec 06 00:01:50 <mail.info> 10.10.10.110: shap postfix/smtpd[22356]: connect from localhost[127.0.0.1]
Dec 06 00:01:51 <mail.info> 10.10.10.110: shap postfix/smtpd[22356]: 0598C6D00E3: client-localhost[127.0.0.1]
Dec 06 00:01:51 <mail.info> 10.10.10.110: shap postfix/cleanup[22359]: 0598C6D00E3: message-id=<20131205230151.0598C6D00E3@shap.ztm.hr>
Dec 06 00:01:51 <mail.info> 10.10.10.110: shap postfix/smtpd[22356]: disconnect from localhost[127.0.0.1]
Dec 06 00:01:51 <mail.info> 10.10.10.110: shap postfix/qmgr[9794]: 0598C6D00E3: from=<logging-server@info-sol.net>, size=621, nrcpt=1 (queue active)
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/smtp[22360]: 0598C6D00E3: enabling PIX workarounds: disable_esmtp delay_dotcrif for ASPMX.L.GOOGLE.COM[173.194.78.27]:25
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/smtp[22360]: 0598C6D00E3: to=<notification@info-sol.net>, relay=ASPMX.L.GOOGLE.COM[173.194.78.27]:25, delay=1.6, delays=0.15/0.13/1.1/0.22, dsn=5.1.1, status=bounced (host ASPMX.L.GOOGLE.COM[173.194.78.27] said: 550-5.1.1 The email account that you tried
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/cleanup[22359]: 9ED416D00E6: message-id=<20131205230152.9ED416D00E6@shap.ztm.hr>
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/bounce[22371]: 0598C6D00E3: sender non-delivery notification: 9ED416D00E6
Dec 06 00:01:52 <mail.info> 10.10.10.110: shap postfix/qmgr[9794]: 9ED416D00E6: from=<>, size=3075, nrcpt=1 (queue active)
```

Follow




First Previous 1 2 3 4 5 Next Last 10

**Note:** Regex merits an entire topic for discussion. For more details on regex please go through this link on [Wikipedia](#). Another thing to be borne in mind is that "Regex matching" matches case sensitive regular expressions if it is set under user's setting (**Login Username -> Settings**) for the variable **web search regex case sensitive**.

### 2.1.3 Notifications in detail

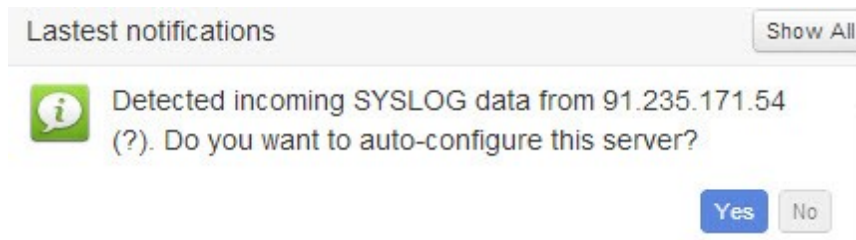
There are three types of notifications. The table below summarizes their properties

Notification Type	Property	Examples
-------------------	----------	----------

	General and Informational	successful PULL copy, successful PUSH copy (syslog,snmp), successfully detected PULL copy time format, new PUSH server autodetected, configuration pending, match on alert rule
	Warnings	failed PUSH copy - no PULL copy method discovered failed PULL copy - autodetect if server didn't receive no PULL data for longer periods of time  push fail ( ), storage usage threshold ( ), failed time format, invalid time format,
	Errors	system alert ( internal <b>OTUS</b> exception) This exception can only be seen by the Superuser role.

**Note:** Autodetect notifications are always on top of others until you confirm them or reject them. Once confirmed **OTUS SIEM** will try to get the server name from server address. If it fails it means there is no DNS entry and therefore a notification of the same. For example if there was a name such as srv1.dobarmail.com then it would mean that the DNS is configured properly and consequently you will not get notifications for that server again. Autodetect works for PUSH copy types (SYSLOG,SNMP)

You can auto-configure a server for incoming SYSLOG data as indicated by a notification shown below. Click **Yes** to auto-configure the server. This is an auto-detect feature used by OTUS to configure the remote server to send data that is not inside the OTUS configuration. This is the fastest way to auto-configure new servers.



**Note:** Please refer the [Creating and Managing Servers](#)<sup>[70]</sup> topic for more information on Auto-Configuration.

Clicking **Show All** opens the following page displaying all notifications of the system assigned to the logged in user's account.

10

Time	Severity	Type	Message	Link
2013-12-05 11:29:06	INFO	JOB_SUCCESS	Copied /var/log/nginx/%-access.log* from server app.imailunlimited.com (1.18 MB) at 2013-12-05 06:59:06	<a href="#">link</a>
2013-12-05 11:09:35	INFO	JOB_SUCCESS	Copied /var/log/nginx/%-access.log* from server app.imailunlimited.com (1.22 MB) at 2013-12-05 06:39:35	<a href="#">link</a>
2013-12-05 11:06:00	INFO	ALERT	Alert alert_200_instance1 (I) at 2013-12-05 00:56:05	<a href="#">link</a>
2013-12-05 11:06:00	INFO	ALERT	Alert alert_200_instance1 (I) at 2013-12-05 00:50:31	<a href="#">link</a>
2013-12-05 11:06:00	INFO	ALERT	Alert alert_200_instance1 (I) at 2013-12-05 00:49:14	<a href="#">link</a>
2013-12-05 11:06:00	INFO	ALERT	Alert alert_200_instance1 (I) at 2013-12-05 00:49:01	<a href="#">link</a>
2013-12-05 11:06:00	INFO	ALERT	Alert alert_200_instance1 (I) at 2013-12-05 00:52:01	<a href="#">link</a>
2013-12-05 11:06:00	INFO	ALERT	Alert alert_200_instance1 (I) at 2013-12-05 00:50:08	<a href="#">link</a>
2013-12-05 11:06:00	INFO	ALERT	Alert alert_200_instance1 (I) at 2013-12-05 00:54:34	<a href="#">link</a>
2013-12-05 11:06:00	INFO	ALERT	Alert alert_200_instance1 (I) at 2013-12-05 00:56:18	<a href="#">link</a>

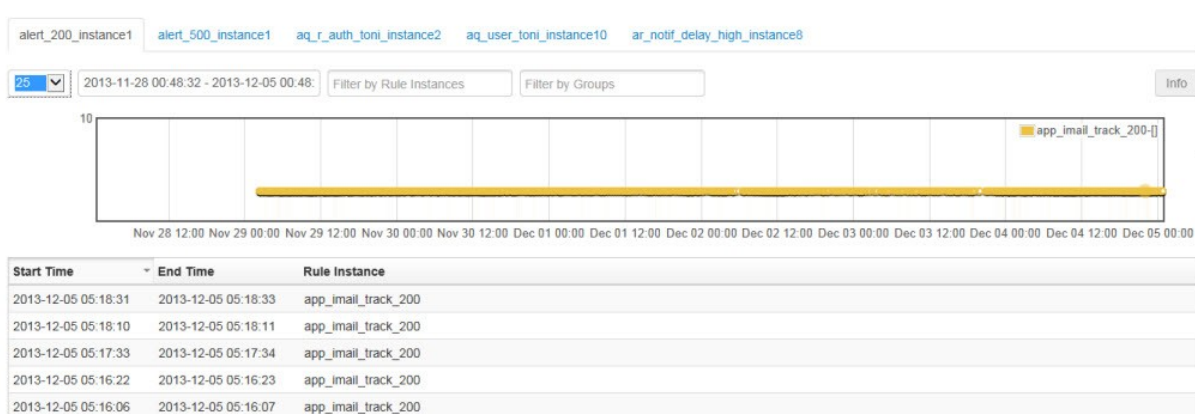
Showing 1 to 10 of 28,978 entries

First Previous 1 2 3 4 5 Next Last

**Note:** The variables **notification web notify alert**, **notification web notify job success**, **notification web notify push success** and **data retention total usage warning limit** under **Configuration -> Settings** are related to the functions of the notifications. Please refer the topic [Managing Settings](#) <sup>[88]</sup> for more details.

### To view Alert type of notifications

1. Click the link for detailed information on that notification. In our example the link of the first alert is clicked. The following page is displayed.



The graph suitably adjusts to display information related to that alert. Information of the same alert at various times and dates appear in the table below. From this page you could skip to other alerts too as can be seen in the various tabs below the selected tab for that particular alert you selected.

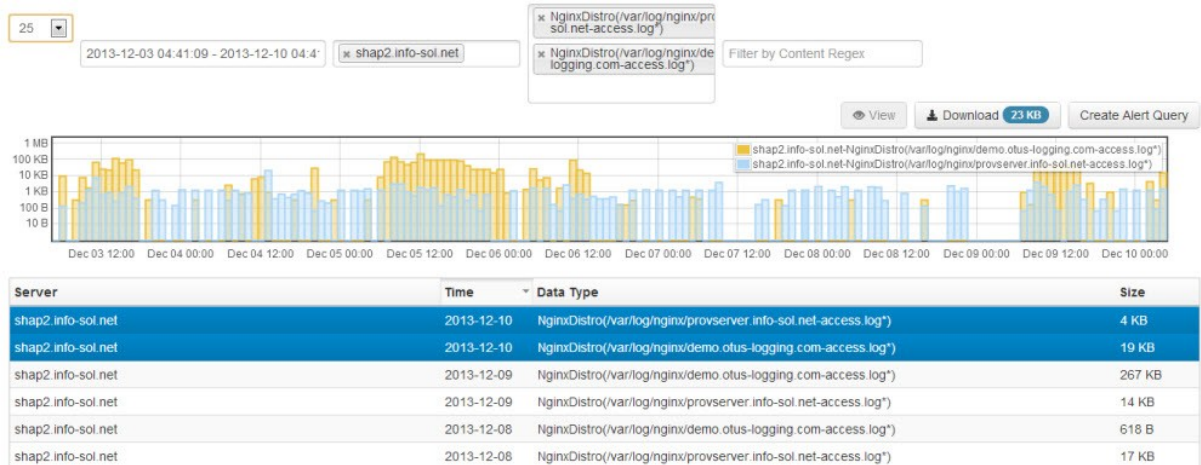
2. Click an alert from this table displays more information as displayed below.

Start Time	End Time	Rule Instance
2013-12-05 20:49:06	2013-12-05 20:49:07	app_imail_track_500
66.219.100.89 - - [05/Dec/2013:16:19:06 -0500] "GET /track/?ip=89-145-108-202&domain_name=siteve1969.com&info= HTTP/1.1" 500 70766 "-" "-" "-"		

**Note:** Depending on the type of notification OTUS responds with various screens. As mentioned earlier in the above example an alert was selected.

### To view a Copy type of notification

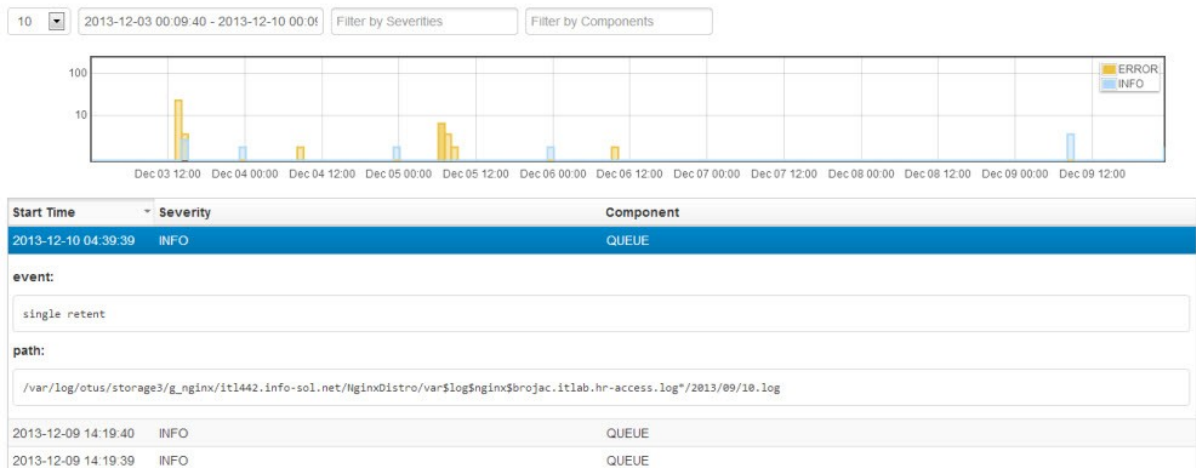
1. Click on a copy type of notification. The following page is displayed displaying more information.



2. Using the filters (explained in the topic [Filtering data using filters](#)<sup>[22]</sup>) more specific data can be searched and fetched.

### To view a system event

1. Click the system event notification from the list of notifications. The following page is displayed.



2. Here too, using the filters (explained in the topic [Filtering data using filters](#)<sup>[22]</sup>) more specific data can be searched and fetched.

# Part



**Data Handling**

### 3 Data Handling

This chapter deals with the data handling functions of the **OTUS, SIEM** such as viewing and downloading logs, searching, indexing etc.,

#### 3.1 Viewing and Downloading raw data


Raw data log files can be viewed, searched (using strings and Regex) and even downloaded. This topic discusses how.

##### To view and logs

1. Click a log file from the table. The selection is highlighted by a blue background bar. The **View** button and **Download** buttons are enabled.

Server	Time	Data Type	Size
app.imailunlimited.com	2013-11-22	NginxDistro(/var/log/nginx/app.imailunlimited.com-access.log*)	1.23 MB
app.imailunlimited.com	2013-11-21	NginxDistro(/var/log/nginx/app.imailunlimited.com-access.log*)	9.78 MB

**Note:** Click the file again to deselect it. The **View** and **Download** buttons are disabled. The last column **Size** indicates the Raw log size. The long path after the log file content denotes the data type. In case you want to share OTUS data with some other systems, it is done outside of system by configuring linux.

2. Click the **View**  button. The contents of the log file are displayed in a new window as shown below.

**Logfile content** g\_imail/app.imailunlimited.com/SecurityDistro/authpriv/2013/12/13.log

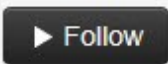
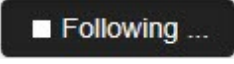
Search ↑ Prev ↓ Next

```

Dec 13 00:01:09 <authpriv.info> 64.79.76.210: d0 sshd[18317]: pam_unix(sshd:session): session closed for user webapps
Dec 13 00:01:23 <authpriv.info> 64.79.76.210: d0 sshd[18445]: Address 85.94.72.179 maps to dns1.ztm.hr, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
Dec 13 00:01:23 <authpriv.info> 64.79.76.210: d0 sshd[18445]: Accepted password for webapps from 85.94.72.179 port 44822 ssh2
Dec 13 00:01:23 <authpriv.info> 64.79.76.210: d0 sshd[18445]: pam_unix(sshd:session): session opened for user webapps by (uid=0)
Dec 13 00:01:24 <authpriv.info> 64.79.76.210: d0 sshd[18447]: subsystem request for sftp
Dec 13 00:03:32 <authpriv.info> 64.79.76.210: d0 sshd[18445]: pam_unix(sshd:session): session closed for user webapps
Dec 13 00:03:39 <authpriv.info> 64.79.76.210: d0 sshd[18523]: Address 85.94.72.179 maps to dns1.ztm.hr, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
Dec 13 00:03:39 <authpriv.info> 64.79.76.210: d0 sshd[18523]: Accepted password for webapps from 85.94.72.179 port 44849 ssh2
Dec 13 00:03:39 <authpriv.info> 64.79.76.210: d0 sshd[18523]: pam_unix(sshd:session): session opened for user webapps by (uid=0)
Dec 13 00:03:39 <authpriv.info> 64.79.76.210: d0 sshd[18525]: subsystem request for sftp

```

▶ Follow First Previous 1 2 3 4 5 Next Last 10 ▾

**Note:** Click  to follow the most recent inputs for this log. Once click the button changes to  and you are immediately repositioned on the last page where you get to see



latest entries being posted in real time on screen instead of you having to close and open the window all the time when new content arrives.

## Functions of the window displaying the log file

### To use text search functionality

1. Type text in the **Search** box located on the top of this window to search the displayed text for matching text entered into the **Search** box.

**Note:** Instead of typing you can even click one or more words from the displayed text and they are input into the **Search** box and marked in the pages as well. Notice in the image below how the word "google" has been searched and marked.

**Logfile content** g\_nginx/shap2.info-sol.net/NginxDistro/var\$log\$nginx\$demo.otus-logging.com-access.log?2013/11/22.log

google

↑ Prev ↓ Next

```
78.3.18.14 - - [22/Nov/2013:09:40:23 +0100] "GET /Otus/Login HTTP/1.1" 200 1170 "http://demo.bitsteer.com/Otus/logs" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
78.3.18.14 - - [22/Nov/2013:09:40:28 +0100] "POST /Otus/openIdLogin?identifier=https://www.google.com/accounts/o8/id HTTP/1.1" 302 0 "http://demo.bitsteer.com/Otus/Login" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
78.3.18.14 - - [22/Nov/2013:09:40:38 +0100] "GET /Otus/openIdLogin?openid.ns=http%3A%2Fspecs.openid.net%2Fauth%2F2.0&openid.mode=id_res&openid.op_endpoint=https%3A%2Fwww.google.com%2Faccounts%2Fopenid.response_nonce-2013-11-22T08%3A40%3A38Z%3BRCQ4mx3OX9w&openid.return_to=http%3A%2Fdemo.bitsteer.com%2Fotus%2FopenIdLogin&openid.assoc_handle=1.AM1YA9XX19ZIN7GfU33H08u9v8cH1PLjituAK80zplX0xtguqREvH99i38MuCRgV5dZrL55ThLhyw&openid.signed-op_endpoint%2Cclaimed_id%2Cidentity%2Creturn_to%2Cresponse_nonce%2Cassoc_handle%2Cns_ext1%2Cext1.mode%2Cext1.type.first_name%2Cext1.value.first_name%2Cext1.type.last_name%2Cext1.value.last_name%2Cext1.type.email%2Cext1.value.email&openid.sig=GP00pp%2F3s9u0Aqf8Rg4Tn7B1eks4dHsf2b3kkyjh7Qk30&openid.identity=https%3A%2Fwww.google.com%2Faccounts%2Fopenid.response_nonce-2013-11-22T08%3A40%3A38Z%3BRCQ4mx3OX9w&openid.claimed_id=https%3A%2Fwww.google.com%2Faccounts%2Fopenid.response_nonce-2013-11-22T08%3A40%3A38Z%3BRCQ4mx3OX9w&openid.mode=fetch_response&openid.ext1.type.first_name=http%3A%2Ffaxschema.org%2FnamePerson%2Ffirst&openid.ext1.value.first_name=Toni&openid.ext1.type.last_name=http%3A%2Ffaxschema.org%2FnamePerson%2Flast&openid.ext1.value.last_name=PivkC480Devic4K87&openid.ext1.type.email=http%3A%2Ffaxschema.org%2Fcontact%2Femail&openid.ext1.value.email=t.pivcevic%40gmail.com HTTP/1.1" 302 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
78.3.18.14 - - [22/Nov/2013:09:40:38 +0100] "GET /Otus/Login?login?openIdLogin=true HTTP/1.1" 302 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
78.3.18.14 - - [22/Nov/2013:09:40:38 +0100] "GET /Otus/logs HTTP/1.1" 200 2781 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
```

2. Now to also search for Mozilla while still displaying google search results click the word "Mozilla" anywhere on this page. The result is as follows.

google|"Mozilla/5.0

↑ Prev ↓ Next

```
78.3.18.14 - - [22/Nov/2013:09:40:23 +0100] "GET /Otus/Login HTTP/1.1" 200 1170 "http://demo.bitsteer.com/Otus/logs" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
78.3.18.14 - - [22/Nov/2013:09:40:28 +0100] "POST /Otus/openIdLogin?identifier=https://www.google.com/accounts/o8/id HTTP/1.1" 302 0 "http://demo.bitsteer.com/Otus/Login" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
78.3.18.14 - - [22/Nov/2013:09:40:38 +0100] "GET /Otus/openIdLogin?openid.ns=http%3A%2Fspecs.openid.net%2Fauth%2F2.0&openid.mode=id_res&openid.op_endpoint=https%3A%2Fwww.google.com%2Faccounts%2Fopenid.response_nonce-2013-11-22T08%3A40%3A38Z%3BRCQ4mx3OX9w&openid.return_to=http%3A%2Fdemo.bitsteer.com%2Fotus%2FopenIdLogin&openid.assoc_handle=1.AM1YA9XX19ZIN7GfU33H08u9v8cH1PLjituAK80zplX0xtguqREvH99i38MuCRgV5dZrL55ThLhyw&openid.signed-op_endpoint%2Cclaimed_id%2Cidentity%2Creturn_to%2Cresponse_nonce%2Cassoc_handle%2Cns_ext1%2Cext1.mode%2Cext1.type.first_name%2Cext1.value.first_name%2Cext1.type.last_name%2Cext1.value.last_name%2Cext1.type.email%2Cext1.value.email&openid.sig=GP00pp%2F3s9u0Aqf8Rg4Tn7B1eks4dHsf2b3kkyjh7Qk30&openid.identity=https%3A%2Fwww.google.com%2Faccounts%2Fopenid.response_nonce-2013-11-22T08%3A40%3A38Z%3BRCQ4mx3OX9w&openid.claimed_id=https%3A%2Fwww.google.com%2Faccounts%2Fopenid.response_nonce-2013-11-22T08%3A40%3A38Z%3BRCQ4mx3OX9w&openid.mode=fetch_response&openid.ext1.type.first_name=http%3A%2Ffaxschema.org%2FnamePerson%2Ffirst&openid.ext1.value.first_name=Toni&openid.ext1.type.last_name=http%3A%2Ffaxschema.org%2FnamePerson%2Flast&openid.ext1.value.last_name=PivkC480Devic4K87&openid.ext1.type.email=http%3A%2Ffaxschema.org%2Fcontact%2Femail&openid.ext1.value.email=t.pivcevic%40gmail.com HTTP/1.1" 302 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
78.3.18.14 - - [22/Nov/2013:09:40:38 +0100] "GET /Otus/Login?login?openIdLogin=true HTTP/1.1" 302 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
78.3.18.14 - - [22/Nov/2013:09:40:38 +0100] "GET /Otus/logs HTTP/1.1" 200 2781 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.114 Safari/537.36"
```

3. Click **Prev** and **Next** buttons to browse all pages of the log file with lines marked with the texts "google" and "Mozilla/5.0". Alternatively you can click the page numbers located at the bottom of the screen or select a page number from the number drop-down list.

First Previous 36 37 38 39 40 Next Last 10

### To use Regex functionality on the page

1. Enter Regex in the **Search** box. The results are highlighted and displayed as explained for the **Text** search.

**Note:** Regex search is explained in more detail in the topic [Filtering data using filters](#)<sup>[22]</sup>.

### To download a log file

When a log file is selected, simultaneously the **Download** button also displays the size of this log file.

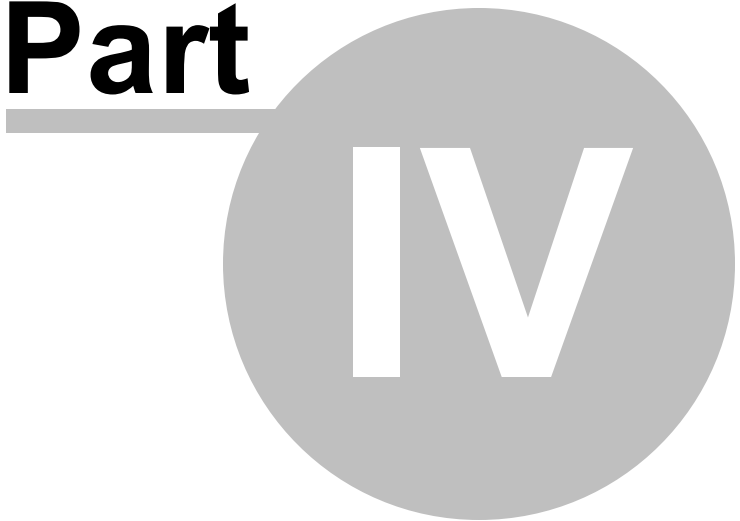


1. Click the **Download** button to download the file. Follow your Internet browser's message to download the file onto your computer.

**Note:** 1. If the file is large, for example over 250 MB then it may take up to 30 minutes to download as it takes time to prepare the download file. In that case when you click the **Download** button the system sends you an e-mail link. Clicking this link will enable downloading of the file that can be done in a separate window of your browser while you can continue your work on **OTUS** uninterrupted. The file size limit of the file that can be downloaded before it is sent for download via the e-mail link is determined by the **web export async size limit (mb)** variable. You can check this variable under **Configuration -> Settings**. In any case you will have to wait for a large download to complete, be that directly from the webapp or from email download link.

2. Regex merits an entire topic for discussion. For more details on regex please go through this link on [Wikipedia](#). Another thing to be borne in mind is that "Regex matching" matches case sensitive regular expressions if it is set under user's setting (**Login Username -> Settings**) for the variable **web search regex case sensitive**.

**Part**



**Indexing log  
search**

## 4 Indexing log search

**OTUS SIEM** offers fast and simple access to relevant data. Indexing is the process where the raw log data is analyzed by an indexer and the important components are extracted and stored in a table form providing for better and concentrated searches to be performed. This yields more meaningful results. About 70+ integrated indexers are available in **OTUS SIEM** from various software and hardware vendors.

Clicking **Indexing** from the **Indexing (menu)** displays the tabs for the various indexers in use currently. You can then load indexed data from a particular indexer by clicking on one of these tabs. The main log area displays the logs related to that particular tab/indexer selected. In the following image the **mail-postfix** indexer has been selected by default and its details reported.

**Note:** The names of indexers (mail-postfix), etc are not constant, they depend on which indexers you use in the Distribution (PULL, SYSLOG, SNMP) indexer column. All currently used indexers are defined here.

Time	Server	msgid	from	to	relay	delay	delays	dsn	status_text	status_info
2013-10-17 06:00:14	host1.genesisvirtual.com	2668B460E0	<admin@genesisvirtual.com>	<rack@host1.genesisvirtual.com>	local	0.66	0.64/0.01/0/0.01	5.1.1	bounced	unknown user: "rack"
2013-10-17 06:00:14	host1.genesisvirtual.com	A14B246144	<>	<admin@genesisvirtual.com>	local	0	0/0/0/0	5.1.1	bounced	unknown user: "admin"
2013-10-17 06:00:14	host1.genesisvirtual.com	2668B460E0	<admin@genesisvirtual.com>	<rack@host1.genesisvirtual.com>	local	0.66	0.64/0.01/0/0.01	5.1.1	bounced	unknown user: "rack"
2013-10-17 05:55:16	host1.genesisvirtual.com	A762946144	<>	<admin@genesisvirtual.com>	local	0	0/0/0/0	5.1.1	bounced	unknown user: "admin"
2013-10-17 05:55:16	host1.genesisvirtual.com	2D0A0460E0	<admin@genesisvirtual.com>	<rack@host1.genesisvirtual.com>	local	0.66	0.64/0.01/0/0.01	5.1.1	bounced	unknown user: "rack"
2013-10-17 05:55:16	host1.genesisvirtual.com	2D0A0460E0	<admin@genesisvirtual.com>	<rack@host1.genesisvirtual.com>	local	0.66	0.64/0.01/0/0.01	5.1.1	bounced	unknown user: "rack"
2013-10-17 05:50:13	host1.genesisvirtual.com	64832460E0	<admin@genesisvirtual.com>	<rack@host1.genesisvirtual.com>	local	0.66	0.64/0.01/0/0.01	5.1.1	bounced	unknown user: "rack"
2013-10-17 05:50:13	host1.genesisvirtual.com	64832460E0	<admin@genesisvirtual.com>	<rack@host1.genesisvirtual.com>	local	0.66	0.64/0.01/0/0.01	5.1.1	bounced	unknown user: "rack"
2013-10-17 05:50:13	host1.genesisvirtual.com	DF47A46144	<>	<admin@genesisvirtual.com>	local	0.01	0/0/0/0	5.1.1	bounced	unknown user: "admin"
2013-10-17 05:45:14	host1.genesisvirtual.com	2D4DF460E0	<admin@genesisvirtual.com>	<rack@host1.genesisvirtual.com>	local	0.66	0.65/0.01/0/0.01	5.1.1	bounced	unknown user: "rack"

As in the case of Indexing if there are more columns that can fit the page, you can use the horizontal scroll-bar at the bottom of the page to scroll left and right to view the hidden columns as can be seen in the image above.

**Note:** When you click on an indexed row one or more raw log lines from which indexed row was constructed is displayed as shown below.

Time	Server	status	dmac	direction	iface	chain	proto	dest	skip	smac	source	dport	sport
2013-12-31 10:49:16	app.mailunlimited.com			DROP	00:0c:28:fd:80		IN		em1	net2fw	TCP	64.79.76.210	

```
Dec 31 06:19:16 <kern.info> 64.79.76.210: d0 kernel: Shorewall:net2fw:DROP:IN=em1 OUT= MAC=d4:ae:52:b2:c:9d:00:0c:cf:28:fd:80:08:00 SRC=66.219.100.89 DST=64.79.76.210 LEN=60 TOS=0x00 PREC=0
```

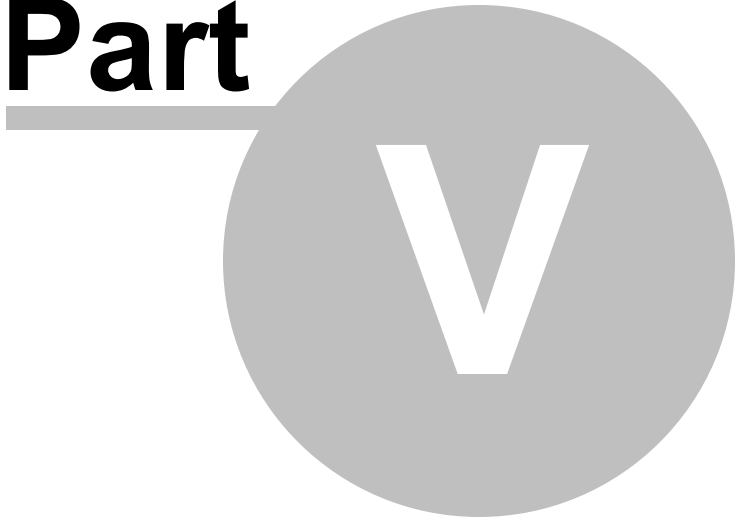
Create Alert Query

For creating an indexed alert query based on search parameters click [Create Alert Query](#). For more information refer the [Create and Managing Alert Queries](#)<sup>[38]</sup> topic.

To use the filters and conditions refer the topic [Filtering data using filters](#)<sup>[22]</sup>.

To use the graph refer the topic [Instant Graph](#)<sup>[20]</sup>.

**Part**



**Alerting**

## 5 Alerting

This chapter deals with creating and managing Alert Queries, Alert Rules and Instances and Alert Events.

There are two types of alerts, raw alerts and alerts on indexed files.

- Raw alerts are created from raw log data and have the type "**raw**" for the indexer name. In them you can write regular expression entries (regex). They can be accessed from this alerting screen or by filtering raw log files ( create alert button on logs screen )

- Indexed alerts are created from indexed log data and have various names under the indexer tab. They can be accessed via the indexing tab also (via the "**create alert query**" button)

It is also to be noted that Alert Queries, Alert Rules and Alert Events are connected. Here's how.

**Note:** **Alerting Queries** and **Alert Rules** are enabled under the **Alerting** menu for a user if the **config\_advanced** role is assigned to the user.

### 5.1 Creating and Managing Alert Queries

As the name indicates Alert Queries are created for querying on data and retrieving information. Alerts are basically raised on indexed columns content and raw log string matches. This topic also explains how to test, modify and delete queries. In alert queries you basically define matches for alerts. This functionality is available only for Superusers (System Administrators)

Alert Queries can be created from here or from Raw log search or Indexer log search.

#### Searching for alerts

Using the **Search**  field you can also search for filters. Just enter a few characters of the filter's name and the page will filter records specific to your input characters or words.

Entering a text such as "authentication" in the search box filters the existing output to filter records displaying the word "authentication" as shown below.

The screenshot shows a search interface with a search box containing 'authentication' and a magnifying glass icon. Below the search box are buttons for '+ Add', 'Delete', and 'Preview'. The main content is a table with columns: Name, Indexer, Filter, and Groups. The table shows two entries filtered by the search term.

Name	Indexer	Filter	Groups
unix_auth_failed_login	unix_auth	operation == "authentication_failure"	server,user
unix_auth_failed_login_total	unix_auth	operation == "authentication_failure"	-

Showing 1 to 2 of 2 entries (filtered from 11 total entries)

Navigation buttons: First, Previous, 1, Next, Last

**Note:** This search feature is available throughout the **OTUS** system wherever a search is required, be that **Users, Roles, Distribution, Groups** etc.,

#### Creating one or more alert queries

1. Select **Alert Queries** from the **Alerting** Menu. The following page is displayed.

10

Name	Indexer	Filter	Groups
app_email_track_200	raw	raw - "track.*200"	-
app_email_track_500	raw	raw - "track.*500"	-
aq_auth_success_totl	raw	raw - "Accepted\s.*\sfor\sstoi"	server
aq_notif_delay_high	mail-postfix	message_id == "<logging-server@info-sol.net>" AND - relay > "0.8"	-
bla	apache	IP == "<bla>"	-
notification_delay_high	mail-postfix	delay LIKE notification@info-sol.net AND relay >= "1.0"	-
unix_auth_accepted_password	unix_auth	operation == "Accepted password"	server,user
unix_auth_accepted_publickey	unix_auth	operation == "Accepted publickey"	server,user
unix_auth_failed_login	unix_auth	operation == "authentication failure"	server,user
unix_auth_failed_login_total	unix_auth	operation == "authentication failure"	-

Showing 1 to 10 of 11 entries

**Note:** Alert queries can also be created wherever the **Create Alert Query** button appears.

Create Alert Query

2. Click the Add  button. The following fields and buttons are displayed. We'll discuss two examples. In our first example we create an alert query for checking all successful logins.

10

Name	Indexer	Filter	Groups
<input type="text"/>	- select -	<input type="text"/> <input type="button" value="Conditions"/>	<input type="text"/>

2. Enter a name for the filter in the **Name** field. For this enter a name from the list of names under the **Name** column. ( For our example enter **unix\_auth\_accepted\_password** ).
3. Select an indexer from the **Indexer** column. Click the box titled - select - under the Indexer column and select an indexer from the list. (For our example select **unix\_auth**)

- select -

apache

bind9\_query

bind9\_query\_with\_timestamp

bind\_query

bind\_query\_with\_timestamp

bind\_response\_checks

bind\_update\_log

4. Click the **Conditions** box under the **Filter** column. The web page displays additional fields as shown below.

5. Click the first drop-down (named - Select -) and from the drop-down select an item. For our example select "**Operation**".

**Note:** Based on the selection made for the **Indexer** column this drop-down can accordingly change showing different values and options. For instance if the file was a raw file then only the following options are available.

The various operators, AND,OR, LIKE also vary for raw log files and indexer log files.

For instance raw log files (as shown in the image above) has the '~' operator for regex matching. For index log files the following operators appear in the drop-down. '=' - equal to, '!=' - not equal to, '<' - less than, '>' - greater than, '<=' - less than or equal to, '>=' - greater than or equal to and the IS NULL and the IS NOT NULL operators.

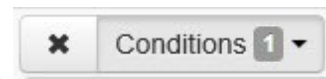
The following are choices when "delay" is selected while making a condition for a filter for Indexer log file.



- Click second box with the down-arrow head and from the drop-down select "==" from the list.



- In the next box enter the words "**Accepted Password**". For our example this means that if the parameter Operation equals the statement "**Accepted Password**" then it means that there is string match for string "Accepted Password" in column operation.

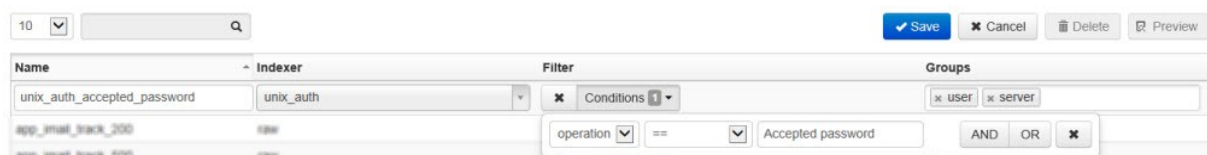


**Note:** In this example we have created only one condition. Note that the number 1 indicates the number of conditions created. We can add one or more conditions. This is discussed in the following section.

- Click the box under the column **Groups** and from the drop-down select one or more groups where this condition needs to be applied. In our example only **servers** and **user** need to be selected.

**Note:** A group is a collection of servers. For raw alerting items can be grouped by server value. For indexed alerting items can be grouped by server value + all other values that are indexed. To find out more about groups and how to create and manage them refer the topic [Creating and Managing Groups](#)<sup>[73]</sup>.

The final image looks as follows.



- Click . The saved condition appears in the list of alerts. To cancel the process click



### Adding one or more conditions


In this example we'll create a filter where we wish to check all logins, both successful or unsuccessful. To do this we simply add one more condition to the existing condition.

- Follow steps 1 to 7 of the previous section.
- Click the **OR** button immediately after creating the first condition. Additional fields are displayed as shown below.

3. Create the second condition as explained in the previous section. This time add the message authentication failure for the second condition. If done correctly you must get the following image.


**Note:** To delete a condition click  associated with that condition.

4. Click the box under the column **Groups** and from the drop-down select one or more groups where this condition needs to be applied. In our example only **servers** and **user** need to be selected.

5. Click . The saved condition appears in the list of alerts.



### To Test an alert query

1. Click the new filter from the list of filters being displayed. The filter is highlighted as shown below.

2. Click . The web page refreshes to display the results of the query.

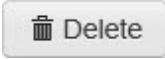
### To modify an alert query

1. Double-click on a field of the query. In our example the Filter field was double-clicked.

2. Modify the field as per requirements and when done click . To quit without saving changes click .

### To delete an alert query

1. Select the alert query to be deleted. It is highlighted with a blue background as seen earlier.

2. Click . The Delete confirmation dialog is displayed.



3. Click **Yes**.

**Caution:** Exercise this function with care. The process cannot be undone. All data is deleted.

## 5.2 Creating and Managing Alert Rules

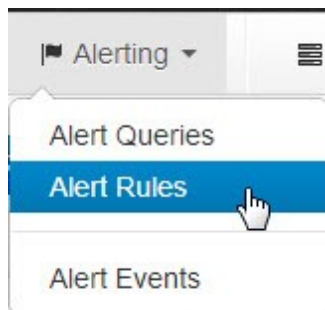
Alert Rules define workflows for various alerting situations and Alert Instances use those Rules applied to servers/groups, alert destinations and N/T values. In this topic creating, modifying and deleting alert rules are discussed. We will then create an instance of a rule.

In alert rules you define how those rules are connected to servers. For this first one defines graphical workflows and then these graphs are connected to instances. There are alert rules applied to specific situations ( servers, N/T, notification destinations). This means that you can create one workflow and connect it to various servers.

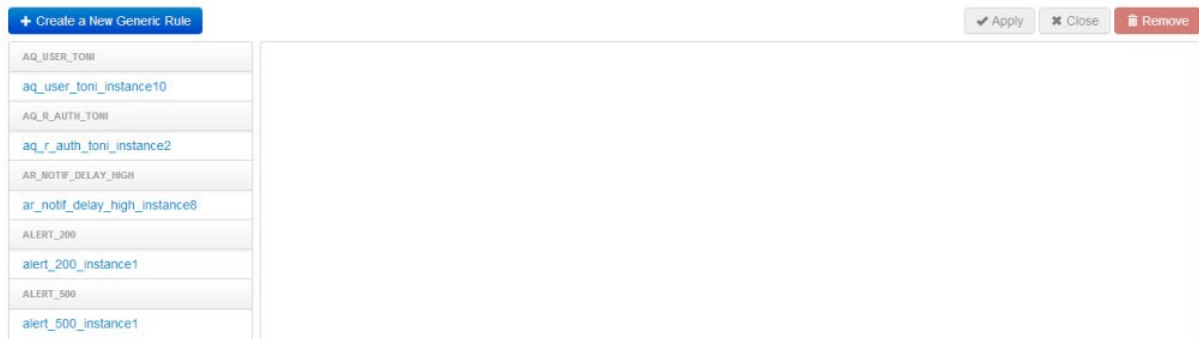
This functionality is available only for System Administrators (Superusers)

### To view the current alerts in the system

1. Click **Alert Rules** from the **Alerting** menu.




The following page opens displaying the current rules in the system.



**Note:** The ones in black color are the rules and the ones in blue under the rules are the instances of the rule. To see the alert instances in action refer to the [Notifications in detail](#)<sup>[27]</sup> topic.

### To create an alert rule

1. Click . The following flow-chart representation is created on the page.



In our example we'll create a new generic rule for unsuccessful logins for a particular user where the user is also notified via the email-address.

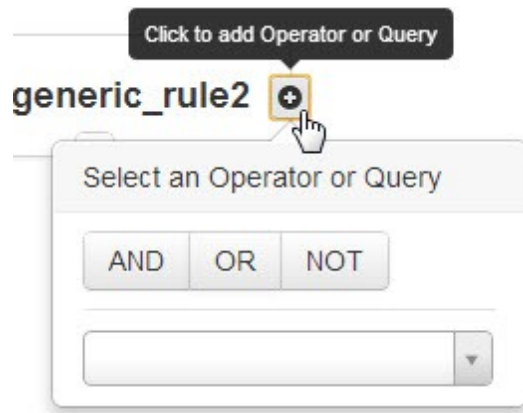
**Note:** You can click and drag this representation to anywhere you want to position it on the work space. Similarly newly added objects can also be similarly moved and the flow-diagram automatically redraws itself.

Also there are **N/T** ( **N** times in **T** period seconds ) before raising alert. This is the way to group entries based on common value ( similar to SQL group by ) so that multiple items can count as one raised alert. **N/T** is that box next to rule i.e. in aq\_user\_toni\_instance10 for example, it is that 1 / 1s box.

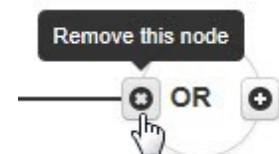


For raw alerting items can be grouped by server value and for indexed alerting items can be grouped by server value + all other values that are indexed

2. Click the **Add Operator or Query** button to add the AND, OR or the NOT condition to the rule as shown below.



3. From the drop-down select **OR**. The resultant image looks as follows.

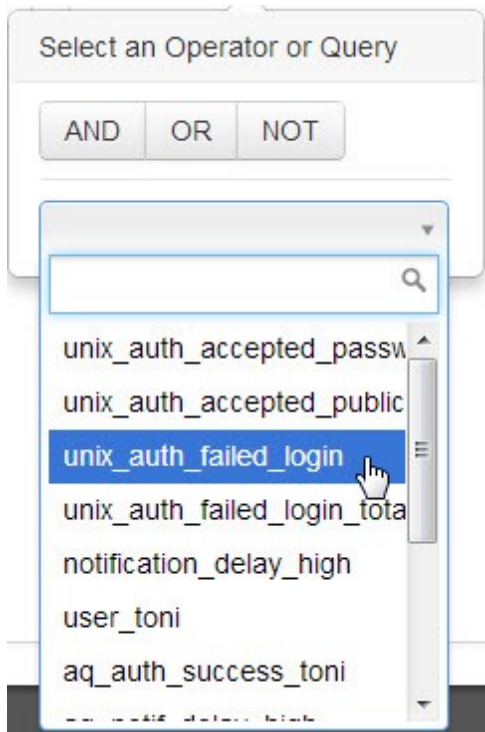


**Note:** If you wish to delete the operator click the **Remove this node** button. A confirmation dialog is displayed as shown below.

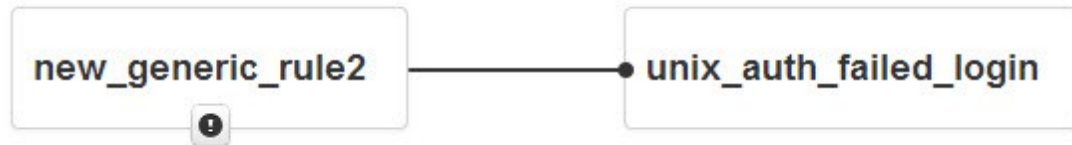


Click **Yes** to remove the node.

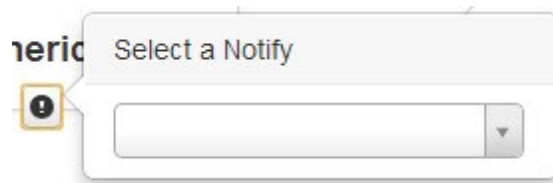
In our case since we wish to notify user when an unsuccessful login takes place, click the Add operator or Query button and select **unix\_auth\_failed\_login** from the drop-down.



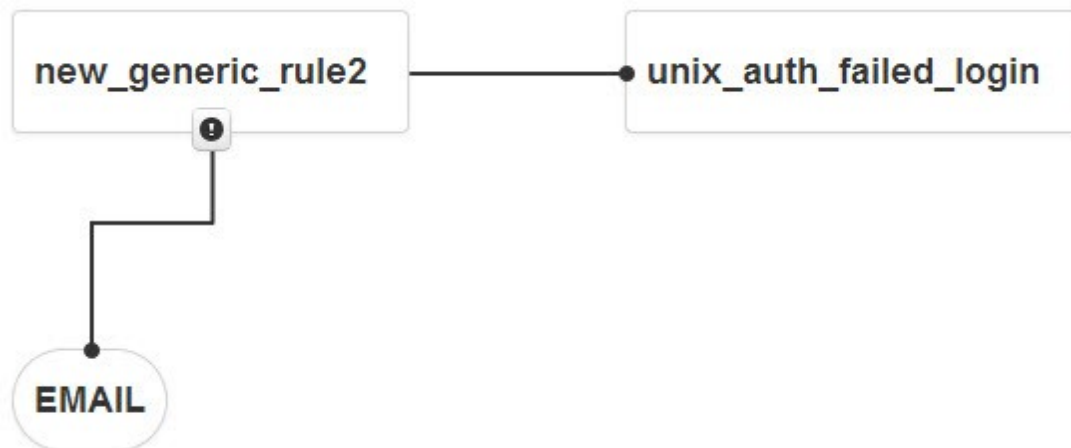
The diagram looks as follows.



4. Click the select a notify button and from the drop-down select email.



The flow-diagram must now look as follows.

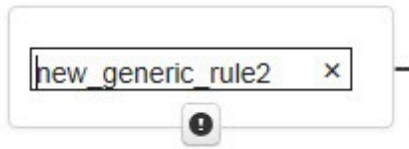


**Note:** In this fashion you can add or remove one or more nodes.

5. Click . The rule is saved and listed in the list of rules on the column on the left as shown below. (NEW\_GENERIC\_RULE\_2)

AQ_USER_TONI
<a href="#">aq_user_toni_instance10</a>
AQ_R_AUTH_TONI
<a href="#">aq_r_auth_toni_instance2</a>
AR_NOTIF_DELAY_HIGH
<a href="#">ar_notif_delay_high_instance8</a>
ALERT_200
<a href="#">alert_200_instance1</a>
ALERT_500
<a href="#">alert_500_instance1</a>
NEW_GENERIC_RULE2

5. Finally to rename the new generic rule double-click the name of the generic rule. It is enabled for editing as shown below.

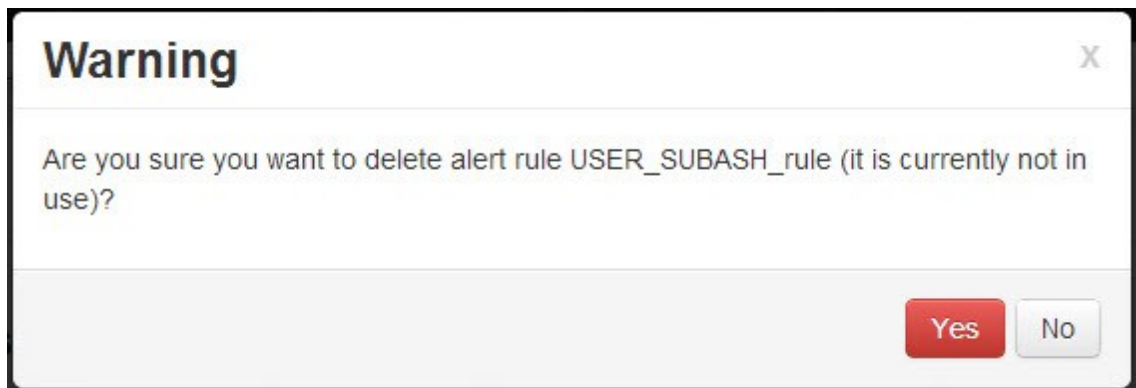


Rename the rule to one of your choice.

6. Click  to save the new name.

### To remove a rule

1. Select a rule from the list.
2. Click . The rule delete confirmation dialog is displayed.



3. Click **Yes**.

## 5.2.1 Creating and Managing Alert Rules > Creating and Managing Rule Instances

Rule instances are created from rules. You can create one or more instances of a rule. Just as with Creating Rules, the Creating Rule Instances functionality is not available to users. It is only available for System Administrators (Superusers). A few examples are discussed below.

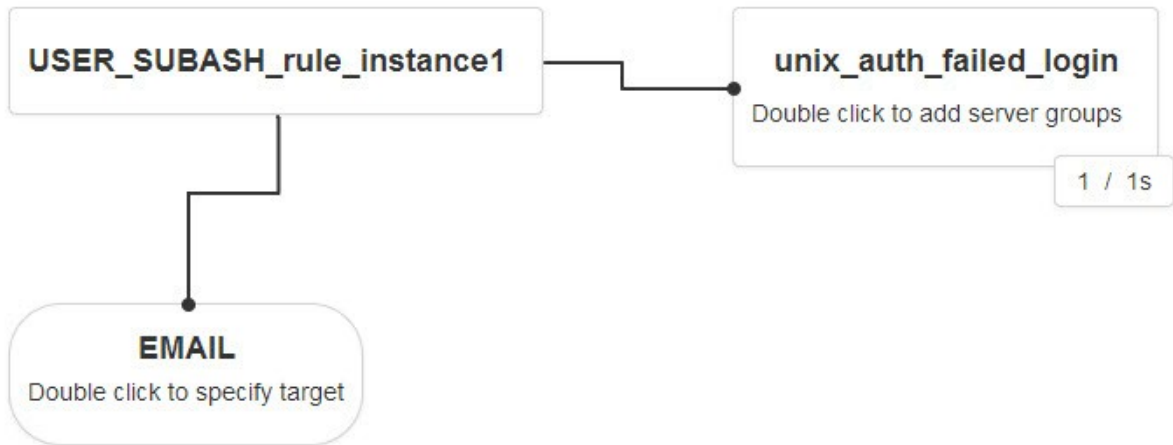
### To create an instance of a rule

1. Click the Add Instance button of the rule from the list as shown below.



The web page uses the diagram from the rule and provides options for adding the required fields as shown below.





**Note:** The N/T ( N times in T period seconds ) specifications apply to instances too.

2. Double click the EMAIL node and in the field enter the appropriate email address.



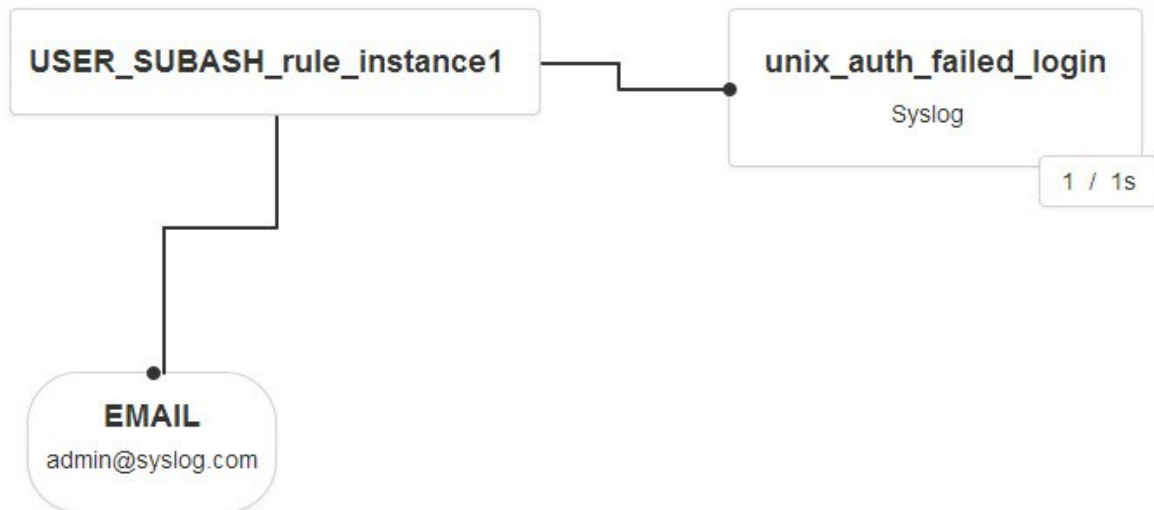
3. Double click the unix\_auth\_failed\_login node and select the suitable server group or groups from the drop-down list.



4. Click  . The rule is created.

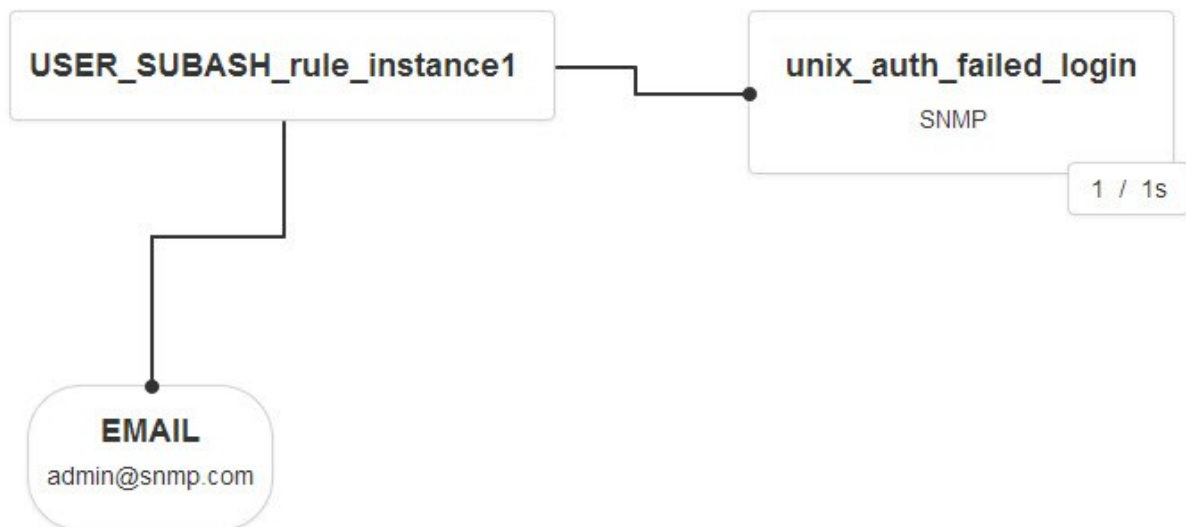
**Example 2** - To create an instance for a failed login rule to apply to a syslog server and to send email to [admin@syslog.com](mailto:admin@syslog.com)

1. Follow the steps outlined in the previous section so that you may get an instance as follows.



**Example 3** - To create instance to apply to an SNMP server and send email to [admin@snmp.com](mailto:admin@snmp.com)


Follow the steps outlined earlier to get the following instance workflow



**Note:** Alert notifications can be syslog, email or snmp.

#### To delete an instance of a rule

1. Select the instance of the rule.

2. Click . The instance delete confirmation dialog is displayed.



3. Click **Yes**.

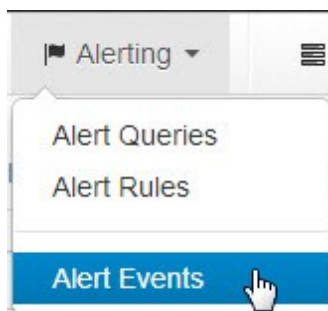
**Caution:** Exercise this function with care. The process cannot be undone. All data is deleted.

## 5.3 Alerting > Viewing Alert Events

Alert events based on instances of Alert Rules created can be viewed using this option. Alert Events show matched alert queries on alert instances. The alert events table is where you see when your alerts matched the rule instances created.

### To view alert events

1. Select **Alert Events** from the **Alerting** menu.



The following page is displayed. The tabs are for the various rule instances.

alert\_200\_instance1 alert\_500\_instance1 aq\_r\_auth\_toni\_instance2 aq\_user\_toni\_instance10 ar\_notif\_delay\_high\_instance8

10 Filter by Date Filter by Rule Instances Filter by Groups info

Start Time	End Time	Rule Instance
2013-12-10 05:26:36	2013-12-10 05:26:38	app_email_track_200
2013-12-10 05:26:30	2013-12-10 05:26:31	app_email_track_200
2013-12-10 05:26:09	2013-12-10 05:26:10	app_email_track_200
2013-12-10 05:23:42	2013-12-10 05:23:43	app_email_track_200
2013-12-10 05:23:34	2013-12-10 05:23:35	app_email_track_200
2013-12-10 05:22:41	2013-12-10 05:22:42	app_email_track_200
2013-12-10 05:21:25	2013-12-10 05:21:26	app_email_track_200
2013-12-10 05:19:46	2013-12-10 05:19:47	app_email_track_200
2013-12-10 05:15:28	2013-12-10 05:15:30	app_email_track_200
2013-12-10 05:13:25	2013-12-10 05:13:26	app_email_track_200

Showing 1 to 10 of 14,534 entries

2. Filter the data using one or more filters. Refer the [Filtering data using filters](#) [22] topic for more information on how to use filters.

3. Click to select a record to view more information as shown below.

Start Time	End Time	Rule Instance
2013-12-10 05:26:36	2013-12-10 05:26:38	app_email_track_200
66.219.100.89 - - [10/Dec/2013:00:56:37 -0500] "GET /track/?ip=115.67.131.146&domain_name=ob1capes.com&info=cy2h1jogRCwgInU101A1U3R1eMuVwFu1IwgImU101A1cZF5zXNAcIBwLXNzLmVb51s1C30IjogF		

4. Click on a rule instance (separated by tabs) to view the alerts of that particular instance.


**Note:** When you click on a matching row, the content that exactly matches in the indexed or raw log file for alert rule is made bold.

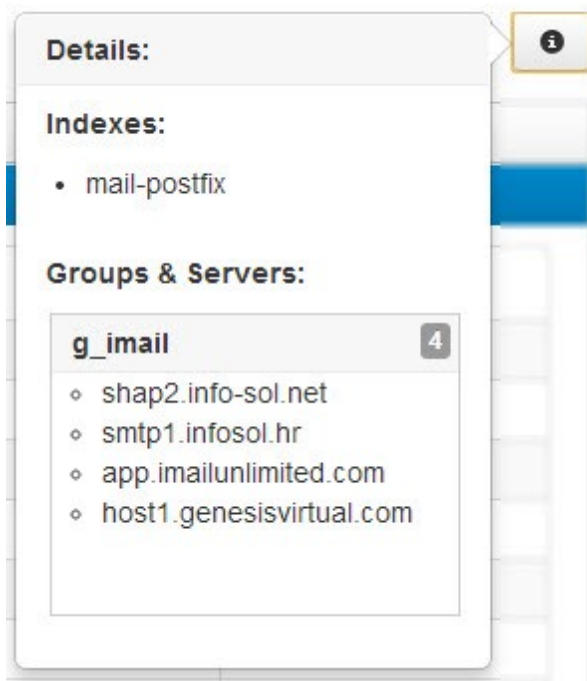
Other types of alerts such as indexed alert events when clicked display the following information.

Start Time	End Time	Rule Instance	servername
2013-12-18 21:04:15	2013-12-18 21:04:16	user_toni	shap2.info-sol.net
<b>time</b>	<b>server</b>		<b>user</b>
2013-12-18 16:34:15	shap2.info-sol.net		toni

and

Start Time	End Time	Rule Instance	server	delay	from
2013-12-18 20:42:42	2013-12-18 20:42:43	aq_notif_delay_high			
<b>time</b>	<b>server</b>		<b>delay</b>	<b>from</b>	
2013-12-18 16:12:43	shap2.info-sol.net		2.9		
2013-12-18 16:12:43	shap2.info-sol.net		2.9		
2013-12-18 16:12:43	shap2.info-sol.net		2.2		
2013-12-18 16:12:43	shap2.info-sol.net		6.9		
2013-12-18 16:12:43	shap2.info-sol.net		3		
2013-12-18 16:12:43	shap2.info-sol.net		6.7		
2013-12-18 16:12:43	shap2.info-sol.net		11		
2013-12-18 16:12:43	shap2.info-sol.net		11		
2013-12-18 16:12:43	shap2.info-sol.net		7.5		
2013-12-18 16:12:43	shap2.info-sol.net		1.2		

You can also get more information by clicking the information button  on the far right.





**Part**



**Reporting**

## 6 Reporting

**OTUS SIEM**, lets you generate a variety of reports. Several of these reports are already built-in into the system. These are the **DEFAULT REPORTS**. However you can always customize a report to suit your needs. These are the **CUSTOM REPORTS**. You can also create a brand new report from scratch. The topics in this chapter show you how.

**Note:** Custom reports are pre-calculated queries for defined period of time. Reports also appear to users depending on their roles. The **report** role ensures the basic reports (bothe **DEFAULT** and **CUSTOM**) are available for a user.

The **DEFAULT REPORT CATEGORIES** are:

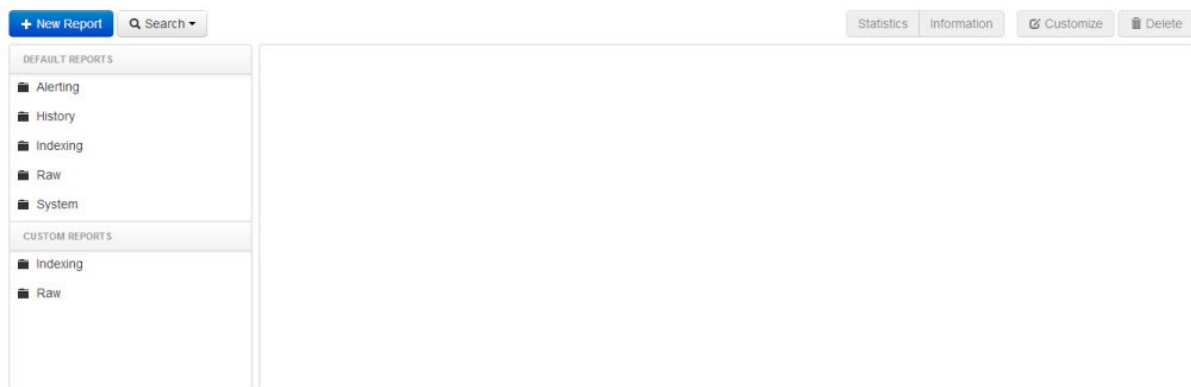
- **Alerting** – reports related to raised raw or indexed alerts
- **History** – internal reports related to otus user login / logout activity
- **Indexing** – reports related to number of indexed entries for a chosen indexer
- **Raw** – reports related to raw log files Some of the raw reports are:

Name of report	Description
Raw_all	size of all raw log files gathered into otus system
Raw_copy_method	size of all raw log files grouped by copy method
Raw_data_type	size of all raw log files grouped by distribution
Raw_default	size of all raw log files grouped by server
Raw_server_copy_method	size of all raw log files grouped by server / copy method
Raw_server	size of all raw log files grouped by server
Raw_storage	size of all raw log files grouped by storage
Raw_storage_ruke	size of all raw log files grouped by storage rule

- **System** – reports related to system errors

### To access the reports

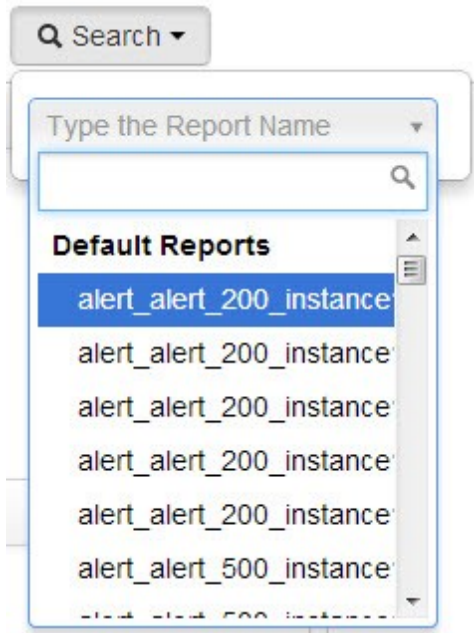
1. Click **Reporting**. The reporting web page is displayed.



### To search for a built-in report and view

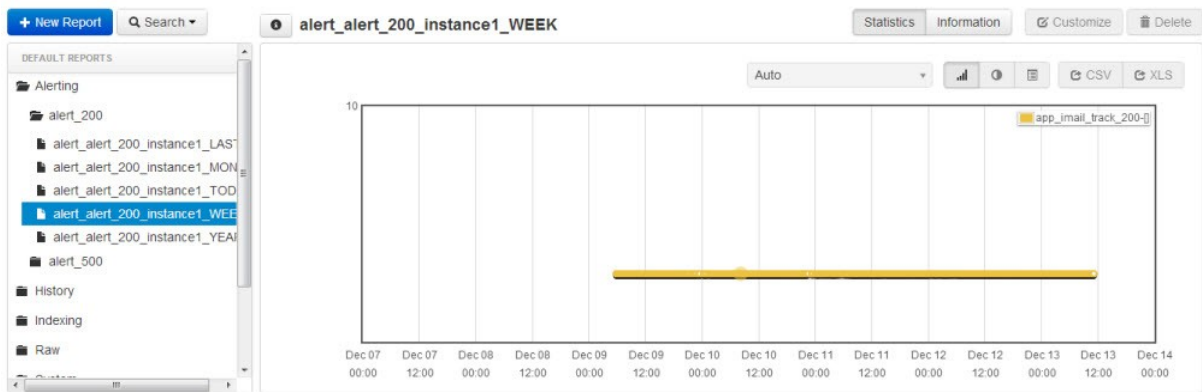


1. Click the **Search** field and select the report from the drop-down list.

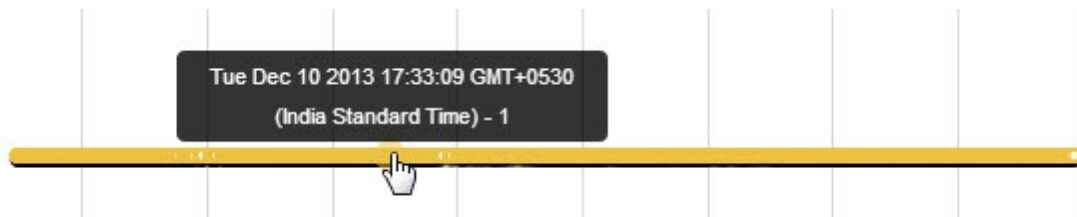


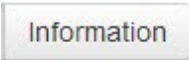
In the example the report alert\_alert\_200\_instance1\_WEEK is selected.

The web page refreshes to display the report shown below.



Pointing mouse on the graph provides more information in call-outs as shown below.



To view information click . The web page refreshes to display the following.

**alert\_alert\_200\_instance1\_WEEK** Statistics Information Customize Delete

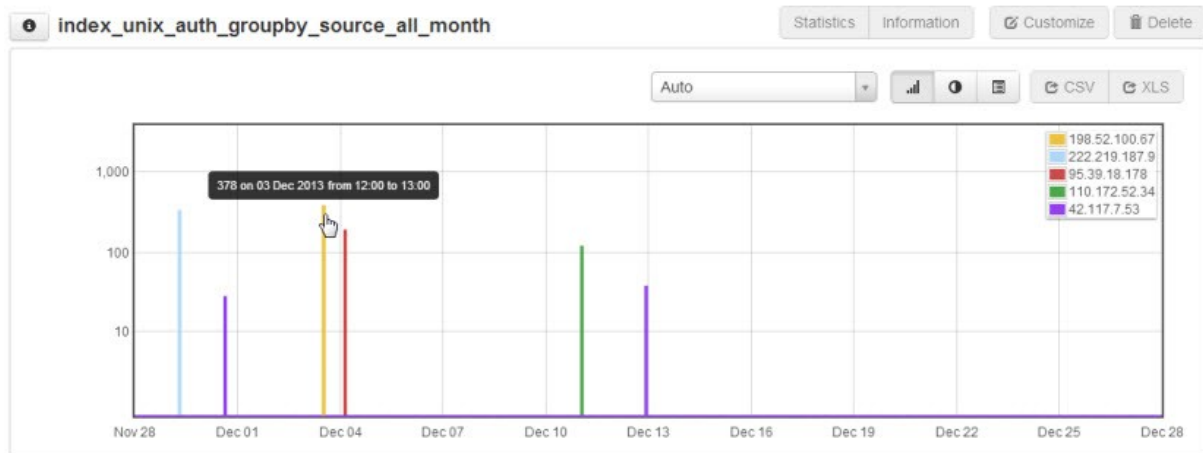
10 CSV XLS

Start Time	End Time	Rule Instance
2013-12-13 15:58:30	2013-12-13 15:58:31	app_email_track_200
2013-12-13 15:58:11	2013-12-13 15:58:12	app_email_track_200
2013-12-13 15:57:37	2013-12-13 15:57:38	app_email_track_200
2013-12-13 15:57:19	2013-12-13 15:57:21	app_email_track_200
2013-12-13 15:56:37	2013-12-13 15:56:38	app_email_track_200
2013-12-13 15:56:17	2013-12-13 15:56:18	app_email_track_200
2013-12-13 15:55:29	2013-12-13 15:55:30	app_email_track_200
2013-12-13 15:54:02	2013-12-13 15:54:03	app_email_track_200
2013-12-13 15:53:17	2013-12-13 15:53:18	app_email_track_200
2013-12-13 15:52:54	2013-12-13 15:52:56	app_email_track_200

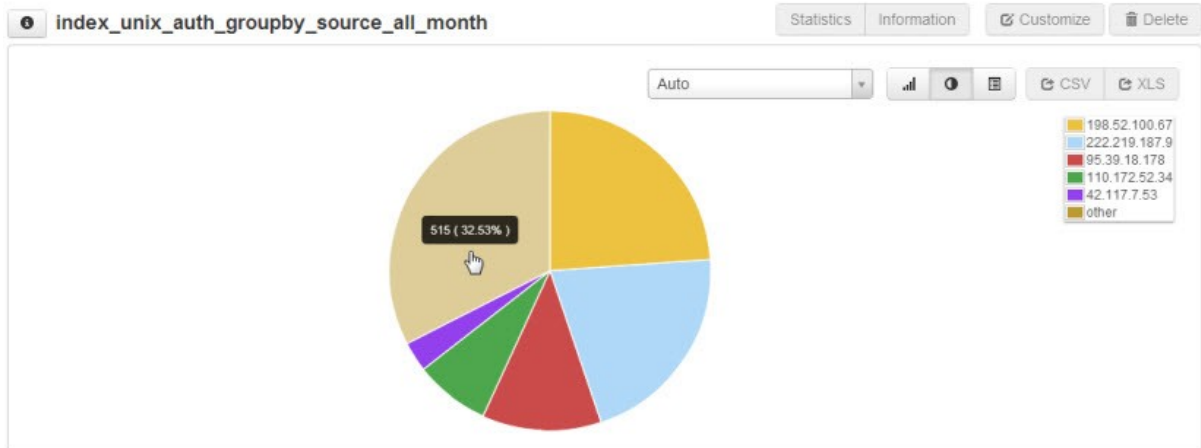
To export the report to CSV or Excel click the button



Also you can view the report in two graphical representations (Bar Graph, Pie and Details). For example here is the image of a report represented by the bar graph.



The same report when viewed by clicking the Pie graph button  displays as follows.

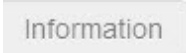


**Note:** Pointing to the graph for the bar or the pie types displays vital information of the report in call-outs as explained earlier in this section.

The same information when the Details button  is clicked displays the following:

The table displays the details of authentication sources. The columns are Time, Label, and Count. The data is as follows:

Time	Label	Count
2013-11-28 04:30:00	198.52.100.67	0
2013-11-28 04:30:00	222.219.187.9	0
2013-11-28 04:30:00	95.39.18.178	0
2013-11-28 04:30:00	110.172.52.34	0
2013-11-28 04:30:00	42.117.7.53	0
2013-11-28 05:30:00	198.52.100.67	0
2013-11-28 05:30:00	222.219.187.9	0
2013-11-28 05:30:00	95.39.18.178	0
2013-11-28 05:30:00	110.172.52.34	0


The Information button  displays details for graph points (example: every login/logout for History -> Auth) as shown below.

history\_auth\_month

Statistics Information Customize De

10 CSV XLS

Time	User	User IP	Action
2013-12-02 10:08:52	root	127.0.0.1	Login
2013-12-02 13:00:44	root	127.0.0.1	Login
2013-12-02 15:19:58	root	127.0.0.1	Login
2013-12-02 15:40:51	root	127.0.0.1	Login
2013-12-02 15:46:35	root	127.0.0.1	Login
2013-12-02 15:52:25	root	127.0.0.1	Logout
2013-12-02 15:52:28	root	127.0.0.1	Login
2013-12-02 15:54:45	root	127.0.0.1	Logout
2013-12-02 15:54:51	root	127.0.0.1	Login

For quick information on a report click the information button  and displays information as shown below.

**Details of:** index\_unix\_auth\_groupby\_source\_all\_month

**Query:** index\_unix\_auth(groupby\_source)

**Date range:** This month

**Groups & Servers:**

All servers 3 ▶

You can also filter the report for ranges as shown below in the Ranges drop-down.

Auto

Hour

Day

Week

Month

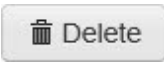
Year

Auto

### To delete a report

**Note:** System reports are not editable or deletable. Only created reports (including customized ones) are deletable.

1. Select the report you wish to delete.

2. Click  **Delete**. The confirmation dialog is displayed.

(not done)

3. Click **Yes**.

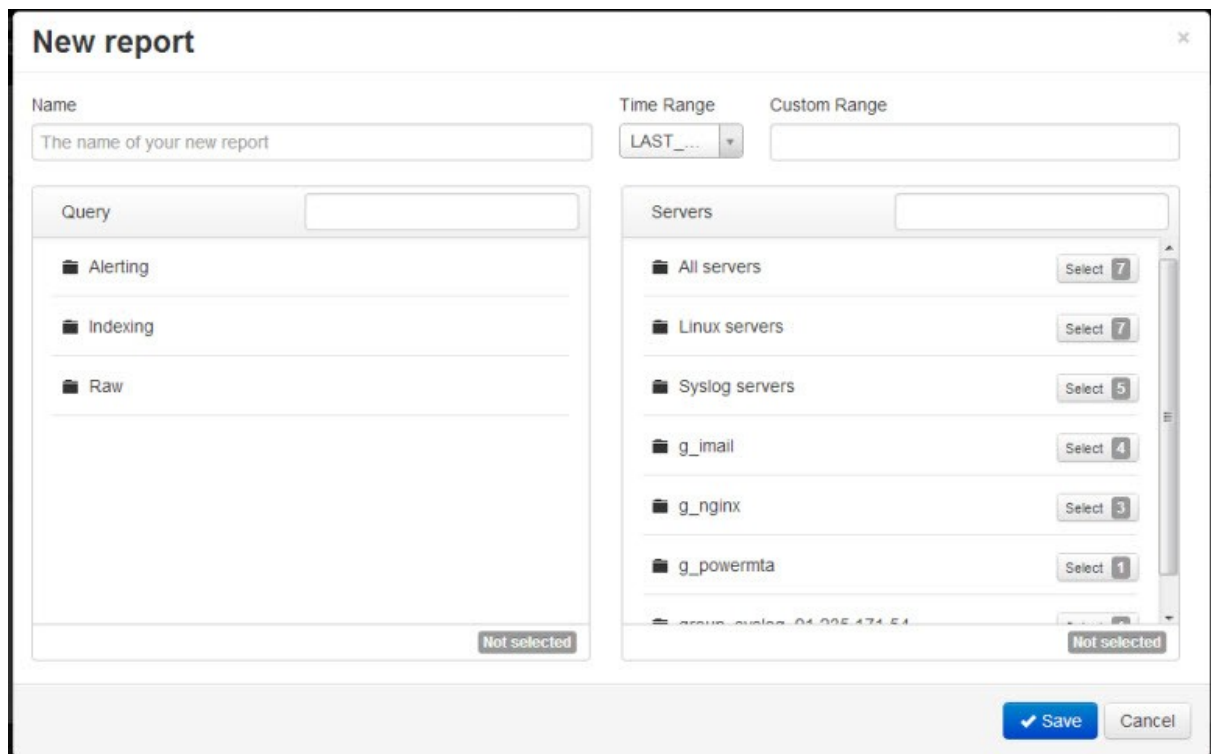
**Caution:** As always delete with care as the process is irreversible.

## 6.1 Creating a report

Besides the default reports you can create your own report using the instances, servers and time periods. This topic shows you how.

### To create a report

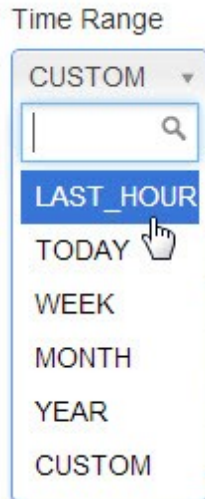
1. Click from the Reporting page. The following pop-up page is displayed.



2. Enter a name for the report in the **Name** field.

For Time, there are two options.

3. Click inside the **Time Range** field and select a time period for the report from the drop-down list.



or

Select **CUSTOM** from the **Time Range** drop-down list, and

Click inside the **Custom Range** field and select a value from the drop-down.

Custom Range

Today

Yesterday

Last 7 Days

Last 30 Days

This Month

Last Month

Custom Range

FROM TO

2013-12-17 2013-12-17

Apply Clear

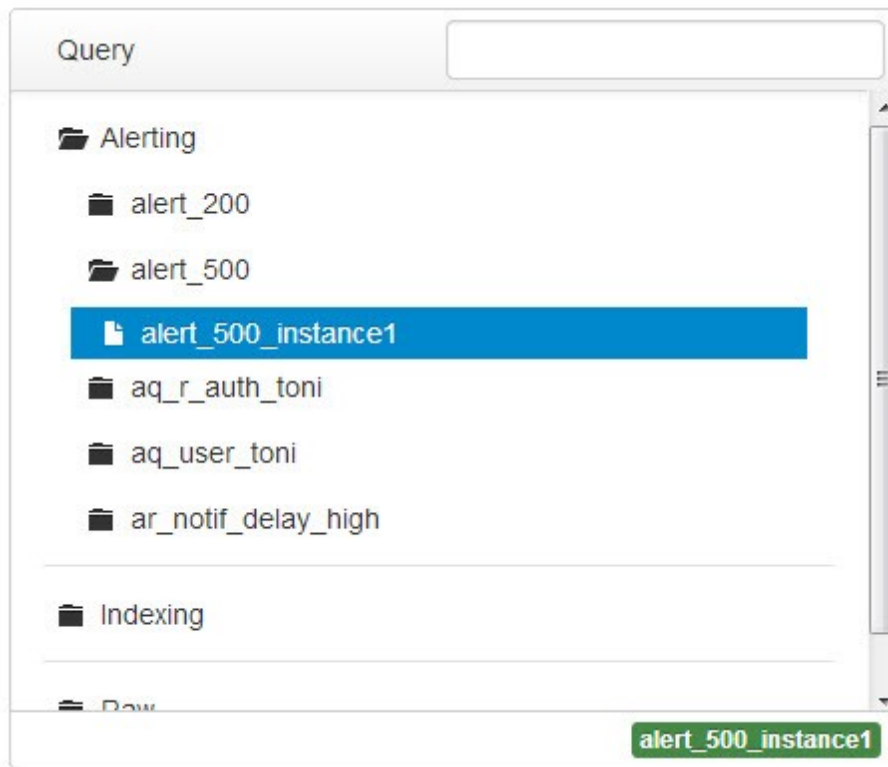
**Note:** Refer the topic [Filtering data using filters](#) <sup>[22]</sup> to learn more selecting a custom time from the **Custom Range** control.

4. Enter a word or characters to search for a query in the **Query** field to locate a query that you want the report to be based upon.

or

Expand the **Alerting**, **Indexing** and **Raw** nodes to locate your query of choice.

Once located select it and it is displayed as shown below.



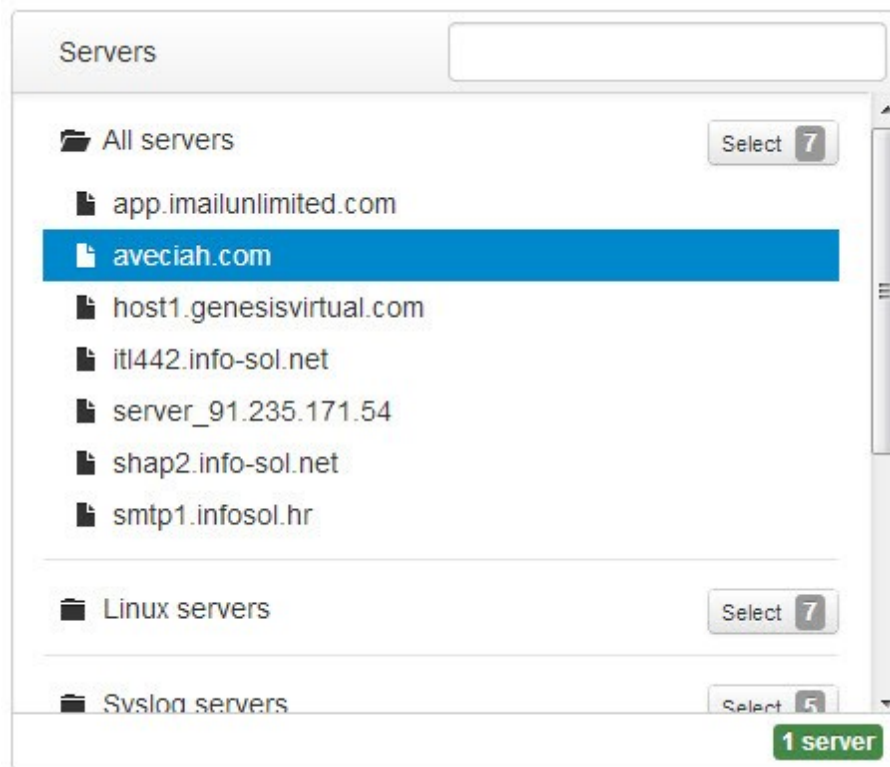
5. Enter a word or characters to search for a server in the **Servers** field to locate a server whose data you want the report to be based upon.

or


Expand the Server nodes to locate your query of choice.

Once located select it and it is displayed as shown below.

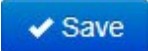




**Note:** Select the server again to deselect it. You may select all servers of a Server Node by clicking the

Select button  of that Server Node. More than one server or Server Node can be selected.

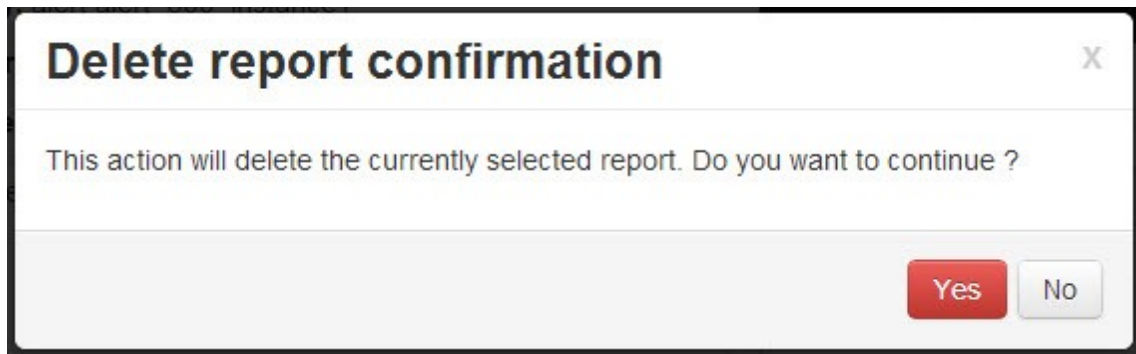
Just like the single server, the Select button  of the Server Node can also be toggled for selecting it or deselecting it.

6. Click . The report is added to the list of reports in the system.

#### To delete such a report

1. Select it from the list of reports.

2. Click . The delete confirmation dialog is displayed.



3. Click **Yes**.

**Caution:** Exercise this function with care. The process cannot be undone. All data is deleted.

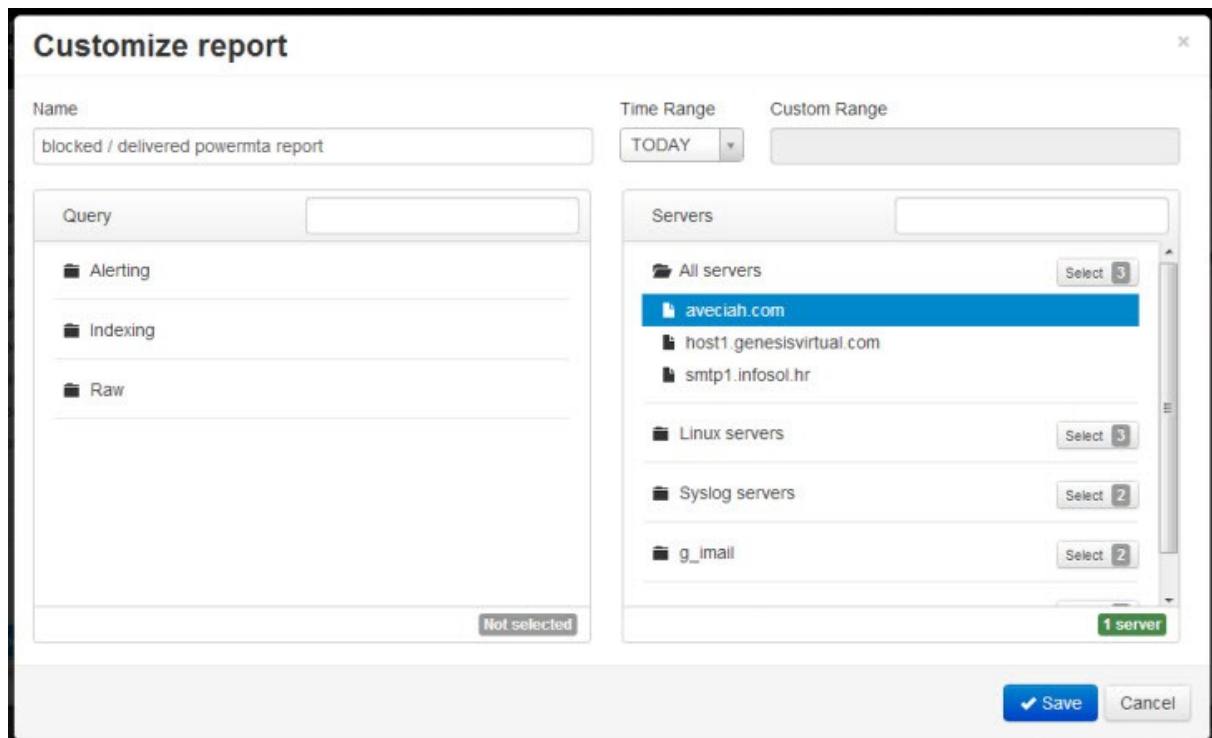
## 6.2 Customizing a Report


You can also customize an existing report. Only **CUSTOM REPORTS** can be customized. **DEFAULT REPORTS** cannot be customized. This topic shows you how.

### To customize a report

1. Search and locate the report under **CUSTOM REPORTS** that needs to be customized.

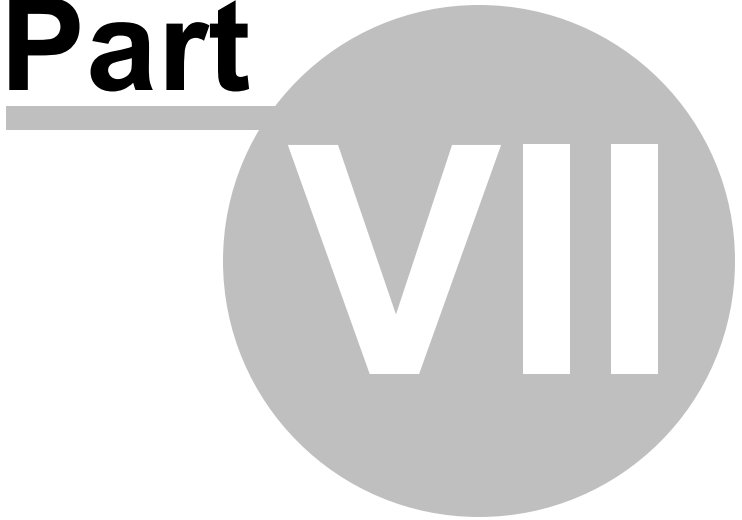
2. Click . The web page now displays the details of the report that you can modify.



- 
3. Modify the report as per you requirements. For more information on how the modify the fields please refer the topic [Creating a report](#)<sup>66</sup>.
  4. Click  when done.



**Part**



**Configuration**

## 7 Configuration

The configuration module helps you perform the following important functions besides others.

- Create users and groups
- Restrict or provide access to the various functionalities of the application
- Tweak system settings

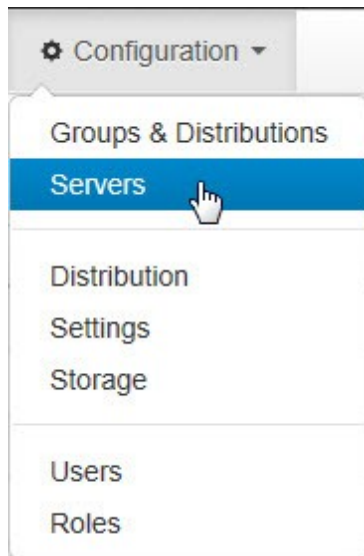
### 7.1 Creating and Managing Servers

This module is where server information is created and stored. **OTUS SIEM** allows you to add and maintain servers. Here you can also track, process and report data and logs extracted from these servers.

The section on **Auto-Detection** and **Copy methods** is located at the bottom of this topic.

**To view the current servers in the system**

1. Select **Servers** from the **Configuration** menu.



The list of servers in the system are displayed in the table below.

Name	IP address	Login	Password	Active	Windows	Groups
app.imailunlimited.com	64.79.76.210	webapps	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g_imail,g_nginx
aveciah.com	66.219.100.89	root	-	<input type="checkbox"/>	<input type="checkbox"/>	g_powermta
host1.genesisvirtual.com	192.237.165.97	-	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g_imail
tl442.info-sol.net	91.235.171.163	webapps	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g_nginx
shap2.info-sol.net	10.10.10.110	logtest	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g_imail,g_nginx
smtp1.infosol.hr	199.175.51.203	webapps	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g_imail

Showing 1 to 6 of 6 entries

**Note:** Using the **Search**  field you can also filter wanted servers.

### To add a server

1. Click . The web page displays the following additional fields and buttons.



The screenshot shows a web interface for adding a server. At the top, there is a search bar with a dropdown menu set to '10' and a search icon. Below the search bar are three buttons: 'Save' (blue with a checkmark), 'Cancel' (grey with an 'X'), and 'Delete' (grey with a trash icon). The main form has a table with the following columns: Name, IP address, Login, Password, Active, Windows, and Groups. The 'Active' column has a toggle switch set to 'ON'. The 'Windows' column has a toggle switch set to 'OFF'. The 'Groups' column has a dropdown menu.

2. Enter the server's name in the **Name** field.
3. Enter the IP address of the server in the **IP address** field.

**Note:** When adding a new server, the hostname, ip address, or both must be specified. The application will attempt to resolve missing information by DNS.

4. Enter the login name of the server in the **Login** field.
5. Enter the password of the server in the **Password** field.
6. Click the ON-OFF toggle control under **Active** to indicate that the server is active. By default it is set to "**ON**".

**Note:** A server that is active means that the server is running. An inactive server means that the server is not in use. An inactive server also does not provide a service or services that it was providing and it also stops utilizing any resources it was using when active.

7. Click the ON-OFF toggle control under **Windows** to indicate the server's configuration status to receive logs from windows server. By default it is set to "**OFF**".

**Note:** When windows switch is turned "ON" the **OTUS** server is configured to receive (PUSH type) event logs from the windows server using the syslog protocol. To forward the needed data, the windows service that must be installed on windows host can be found here <https://code.google.com/p/eventlog-to-syslog/>. By turning on this switch the data type for windows server in the raw log search is sorted by event log type (security,application type etc).

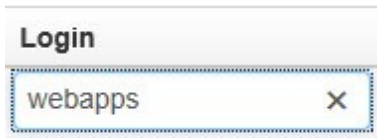
8. Click inside the **Groups** box to choose one or more groups from the drop-down list.



**Note:** You can search for groups by typing the first few characters of the group's name. To delete a server from the **Groups** box after it has been selected, click the "**X**" symbol of the group to remove it from the field.

9. Click  to save the record.

### To modify a server's information

1. Double-click the field that needs to be modified and the field is enabled for editing as shown below. In the example below the **Last name** field of a server was double-clicked.



2. Modify the field and click  to save the changes. Click  to quit without saving the changes.

### To delete a server from the system

1. From the list of servers displayed (refer step 1 of the first section of this topic) select the server you wish to delete. The selected server is highlighted as shown below.



2. Click . The delete confirmation dialog is displayed.



3. Click **Yes**.

**Caution:** Exercise this function with care. The process cannot be undone. All archived data (raw logs, indexed logs, reports) for that server are deleted.

### OTUS Copy methods

There are two types of copy methods in **OTUS** that use the following processes.

1. **PULL METHOD** - Here the server gets files by requesting them from the remote server. Otus periodically fetches new data from remote servers via SCP, FTP and HTTP.
2. **PUSH METHOD** - Here the server receives files from the remote server. Remote servers send data to OTUS in real time via SYSLOG or SNMP.

### Auto-detecting PULL copy method



There is no way to select PULL copy method for each server, only username and password are entered. **OTUS** automatically tries all available copy methods and uses one that:

- successfully logins
- successfully transfers file from remote server

Priorities for PULL are the following:

1. SCP
2. FTP
3. HTTP

### **Auto-detecting PUSH copy method**

The easiest way to configure OTUS for receiving files is just to configure remote servers to send SYSLOG or SNMP data to the **OTUS** server. When **OTUS** detects a new source of data it will present an auto-detection confirmation dialog. When and if a system administrator confirms it, the new server will become configured with smart defaults and will be ready to use.

If auto-configuration is allowed it will try to auto-configure new server with:

1. server information (server name, ip address, custom group)
2. connecting the server to groups and distributions

## **7.2 Creating and Managing Groups & Distributions**

Group is a collection of servers and when we create a group they are linked to distributions. All configuration, reporting, etc., is defined on groups and not on single servers.

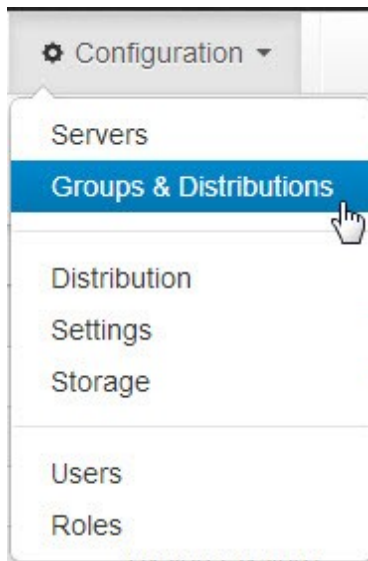
Server -

Distributions that contain multiple paths describe how the log file data is going to be stored. While connecting groups and distributions we are basically connecting the various servers of that group the distribution methods. This topic explains groups, how to create them and manage them.

A DistributionGroup is a link between a distribution and a group.

### **To view existing groups**

1. Select **Groups and Distributions** from the **Configuration** menu.




The following page is displayed.

Group	Distribution
g_mail (4)	PostfixDistribution (syslog)
g_mail (4)	SecurityDistro (syslog)
g_nginx (3)	NginxDistro (pull)
g_powermta (1)	PowerMTA (pull)
group_syslog_192.237.165.97 (0)	Syslog (syslog)
group_syslog_91.235.171.54 (1)	Syslog (syslog)


Showing 1 to 6 of 6 entries

### To add a group

1. Click . The following fields and buttons are displayed.

Group	Distribution
- select -	- select -

Buttons: Save, Cancel, Delete

3. Click inside the **Group** field and select a group from the drop-down list.
4. Click inside the **Distribution** field and from the drop-down select a distribution.
5. Click . The new group is created and it is added to the list of groups in the table.

### To modify a group and adjust settings

1. Click a record of a group from the table. The servers of that group and their settings are displayed.

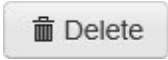
Group	Distribution	Copy	Index
g_email (4)	PostfixDistribution (syslog)	<input type="checkbox"/>	<input type="checkbox"/>
g_email (4)	SecurityDistro (syslog)	<input type="checkbox"/>	<input type="checkbox"/>
AUTH		<input type="checkbox"/>	<input type="checkbox"/>
AUTHPRIV		<input type="checkbox"/>	<input type="checkbox"/>
KERN		<input type="checkbox"/>	<input type="checkbox"/>

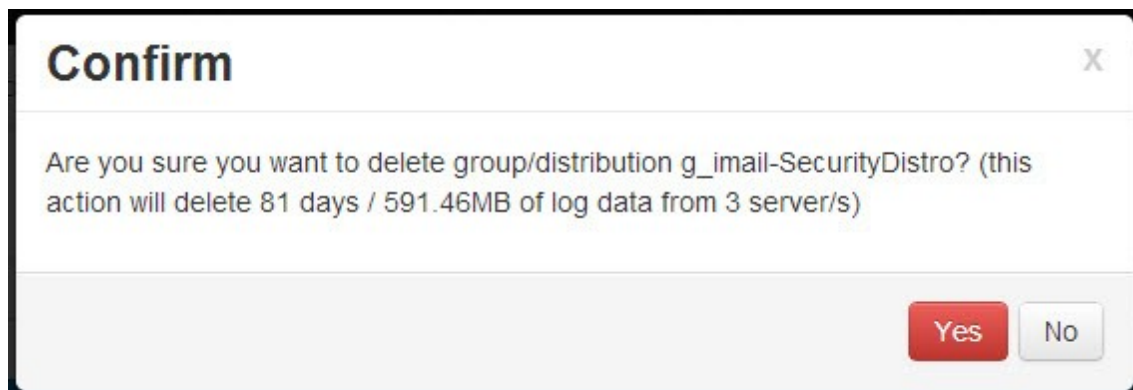
- Click the ON/OFF toggle switch for **Copy** or **Index** as per requirement. The settings are changed.

**Note:** As the name indicates the **Copy** button allows you to copy that entry and the **Index** button allows you to index the entry.

- Click  to save the changes. Click  to close without saving any changes made.

### To delete a group

- Click to select the record of a group that is to be deleted.
- Click . The delete confirmation dialog is displayed.



- Click **Yes** to delete the record.

**Caution:** Exercise this function with care. The process cannot be undone. All data is deleted.

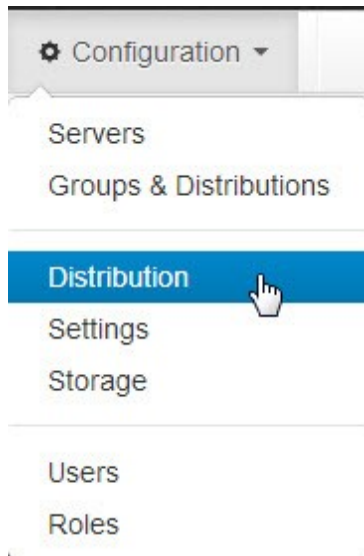
## 7.3 Creating and Managing Distribution

A Distribution defines the information that is available/required on a remote server. This is used so a pull copy method knows what data to expect on & copy from a remote server. This is used by a push copy method to know what data to expect to receive from a remote server. It defines if additional steps (indexing) should be done on the incoming data.

Distributions are of three types, **Pull**, **SYSLOG** and **SNMP**. This topic and their sub-topics discuss the various distributions and how to create, modify and delete them.

To view the distributions

1. Select **Distribution** from the **Configurations** menu.



The following page is displayed.

Pull Distribution   Syslog Distribution   SNMP Distribution

10

Distribution	Path	Timeformat	Indexers
AlertDistribution	/var/log/otustestdata/custom/alertboom/log	%b %d %H.%M.%S	-
NginxDistro	/var/log/nginx/%-access.log*	%C	-
PowerMTA	/var/log/pmta/acct-%*.csv	%Y-%m-%d %H.%M.%S	powermta

Showing 1 to 3 of 3 entries

First Previous 1 Next Last

To view the distributions under the other tabs (**Syslog** and **SNMP**) click them.


### 7.3.1 Pull Distribution

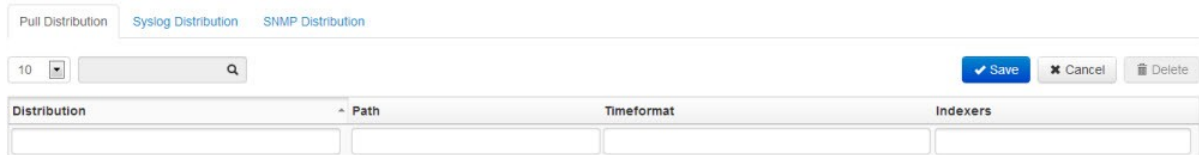
This topic deals with the creation and management of PULL distributions in the system. As the name suggests PULL distribution involves "pulling" or extraction of data from remote servers. The major protocols used here are HTTP, SCP and FTP.

The time format that is used for recognizing time in the file is fetched with PULL. If this time format is left empty the system will try to auto-detect the remote time format. This is used to sort files by date for instance in raw log search.

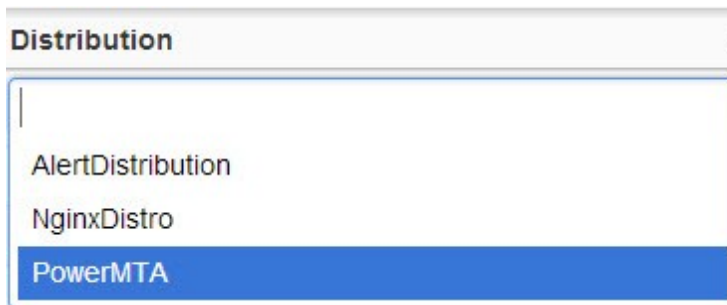
**To create a PULL distribution**

1. Ensure you are the PULL distribution page. Refer parent topic [Creating and Managing Distribution](#) for details.

2. Click . The following fields and buttons are displayed.



3. Click inside the **Distribution** field and select a distribution from the drop-down list. This is a suggest drop-down. Here you can select an existing distribution name (this means adding a new path to an existing distribution) or create a new one.



4. Enter a path in the **Path** field.

**Note:** "\*" groups all files into the same distribution. For example: for /var/log/\*.log /var/log/a.log and /var/log/b.log are copied to same distribution path. '%' groups all files into different distributions for example, for /var/log/%-access.log /var/log/www.host1-access.log and /var/log/www.host2-access.log will be copied to different distributions making it possible to store each file into different distribution path.

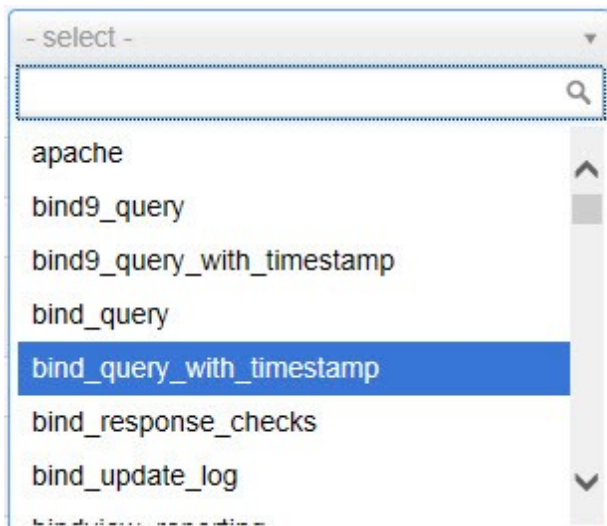
A distribution path can contain wildcards. The following table explains the behavior of wildcards in more detail.

Wildcard character	Behavior	Example
"*"	Tells <b>OTUS</b> to copy everything that is matched by it. Useful when copying a large or variable amount of log files from a remote server.	To easily copy rotated log files - /var/log/auth.log*, as it matches all required remote files: /var/log/auth.log,/var/log/auth.log.1,/var/log/auth.log.2, etc.
"%"	Useful when various remote paths are to be matched, but are to be stored in the system separately, as they are completely different log types.	An example path to easily copy all access log files is /var/log/%-access.log, that matches all access log files but stores them separately in the system. This path will match remote files: /var/log/host1-


		access.log, /var/log/host2-access.log, etc.
Using "*" and "%" in combination.	A combination of the behavior of both the wildcards.	/var/log/%-access.log* matches: /var/log/host1-access.log, /var/log/host1-access.log.1, /var/log/host2-access.log, /var/log/host2-access.log.2. And stores this data separately for each host.

5. Enter a time format in the **Timeformat** field. Refer the topic [List of OTUS time formats](#)<sup>[120]</sup> for more information.

6. Click inside the **Indexers** field and from the drop-down select one or more indexers. You can search for an indexer by entering characters or words of the name of the indexer in the empty field located on drop of the drop-down list. To remove an indexer click the "X" of the name of the indexer.

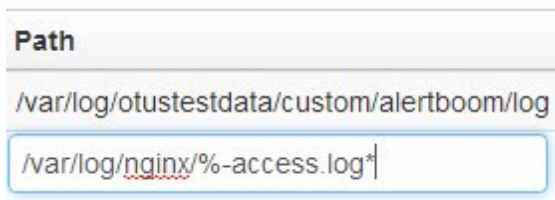


**Note:** Indexers are optional, if none is entered only raw log files are stored on server.

7. Click . The new distribution is added to the list of distributions in the table.

### To modify a PULL distribution

1. Double-click an editable field of a record in the table and it is enabled for editing. In the example the **Path** field of a record has been double-clicked.



Path

/var/log/otustestdata/custom/alertboom/log

/var/log/nginx/%-access.log\*

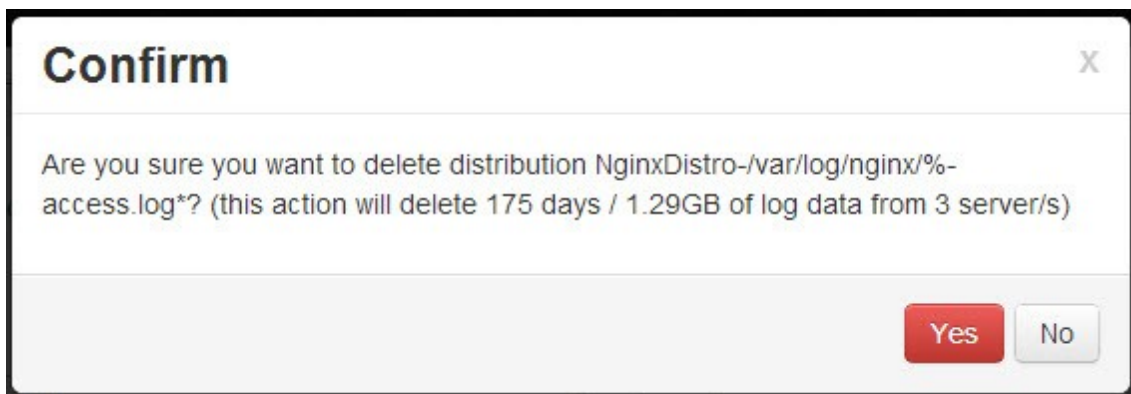
2. Edit the field as required.

3. Click  to save the changes. Click  to close without saving any changes made.

### To delete a PULL distribution

1. Click to select the record of a PULL distribution to be deleted.

2. Click . The delete confirmation dialog is displayed.



**Confirm** X

Are you sure you want to delete distribution NginxDistro-/var/log/nginx/%-access.log\*? (this action will delete 175 days / 1.29GB of log data from 3 server/s)

**Yes** **No**

3. Click **Yes** to delete the record.

**Caution:** Exercise this function with care. The process cannot be undone. All data is deleted.

## 7.3.2 SYSLOG Distribution

This topic deals with the creation and management of SYSLOG distributions in the system. The SYSLOG is a standard for computer message logging.

### To create a SYSLOG distribution

1. Ensure you are the PULL distribution page. Refer parent topic [Creating and Managing Distribution](#)<sup>75</sup> for details. If you have done it correctly the following page is displayed.

Pull Distribution Syslog Distribution SNMP Distribution

10

Distribution	Facility	Indexers
PostfixDistribution	Mail	mail-postfix
SecurityDistro	Kern	network-shorewall
SecurityDistro	Auth	system-ssh,unix_auth
SecurityDistro	Authpriv	system-ssh,unix_auth
Syslog	All	
Syslog2	All	catchall_syslog,catchall_syslog_wrapped
Syslog2	Auth	unix_auth

Showing 1 to 7 of 7 entries

2. Click . The following fields and buttons are displayed.

Pull Distribution Syslog Distribution SNMP Distribution

10

Distribution	Facility	Indexers
<input type="text"/>	<input type="text" value="- select -"/>	<input type="text"/>

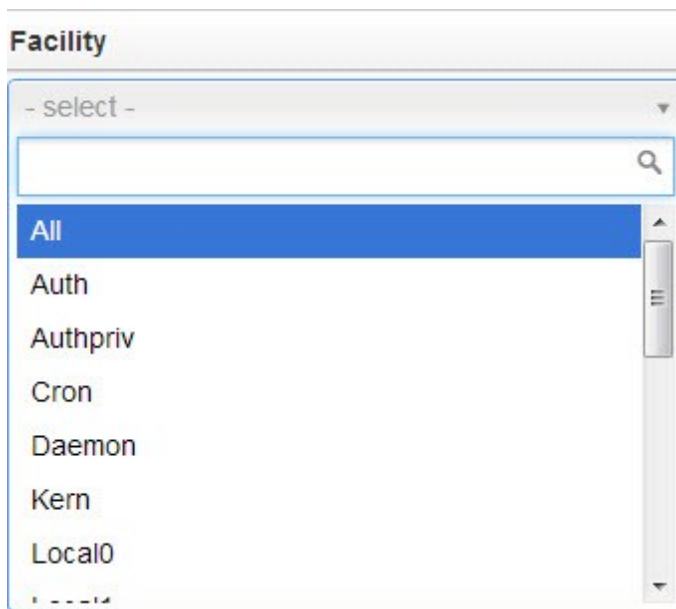
3. Click inside the **Distribution** field and select a distribution from the drop-down list. This is a suggest drop-down. Here you can select an existing distribution name (this means adding a new path to an existing distribution) or create a new one.

**Distribution**

- PostfixDistribution
- SNMP
- SNMP2
- SecurityDistro
- Syslog
- Syslog2

4. Click inside the Enter a path in the **Facility** field and select a facility from the drop-down list.



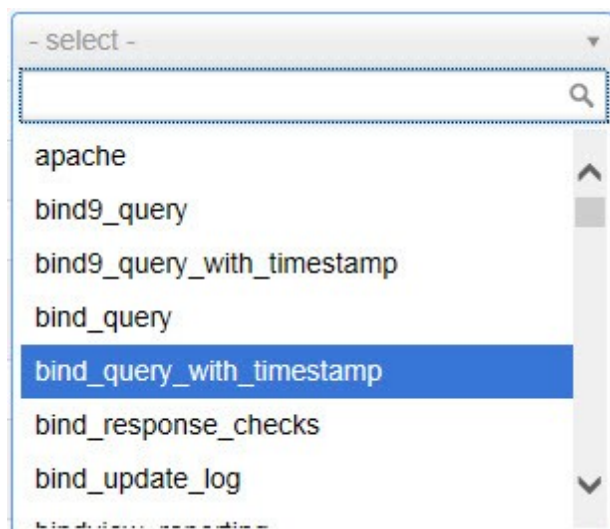


**Note:** A SYSLOG distribution consists of one or more facilities, a distro & group links groups to distributions. When **OTUS** receives a syslog message it does the following:


- finds the server by the syslog message remote ip addr
- finds all the servers groups
- for each group it finds all the associated SYSLOG distros (by the group & distro link)
- for each SYSLOG distro, it looks at the defined facilities
- it only accepts SYSLOG messages with facilities that are defined in this distro
- optionally if the distro/facility was assigned an indexer it indexes the data with that indexer

You can also have 2 different syslog distros with the same facility, and for example one is indexed and one is not.

6. Click inside the **Indexers** field and from the drop-down select one or more indexers. You can search for an indexer by entering characters or words of the name of the indexer in the empty field located on drop of the drop-down list. To remove an indexer click the "X" of the name of the indexer.

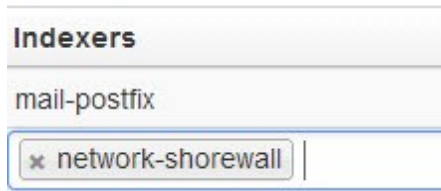


**Note:** Indexers are optional. If none is entered only raw log files are stored on server.

7. Click . The new distribution is added to the list of distributions in the table.

#### To modify a syslog distribution

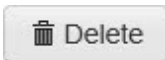
1. Double-click an editable field of a record in the table and it is enabled for editing. In the example the **Indexers** field of a record has been double-clicked.

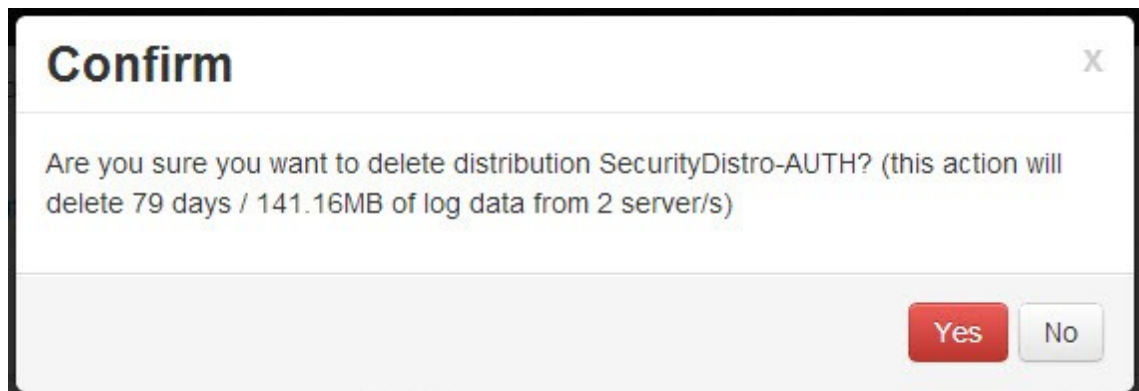


2. Edit the field as required.

3. Click  to save the changes. Click  to close without saving any changes made.

#### To delete a syslog distribution

1. Click to select the record of a Syslog distribution to be deleted.
2. Click . The delete confirmation dialog is displayed.



3. Click **Yes** to delete the record.

**Caution:** Exercise this function with care. The process cannot be undone. All data is deleted.

### 7.3.3 SNMP Distribution

This topic deals with the creation and management of SNMP distributions in the system. Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks".

#### To create a SNMP distribution

1. Ensure you are the SNMP distribution page. Refer parent topic [Creating and Managing Distribution](#) <sup>75</sup> for details. If you have navigated correctly the following page is displayed.



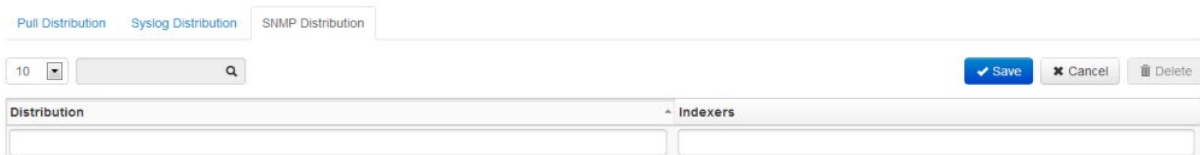
The screenshot shows the 'SNMP Distribution' page with a table containing two entries:

Distribution	Indexers
SNMP	
SNMP2	catchall,catchall_snmp

Showing 1 to 2 of 2 entries

Navigation buttons: First, Previous, 1, Next, Last

2. Click . The following fields and buttons are displayed.

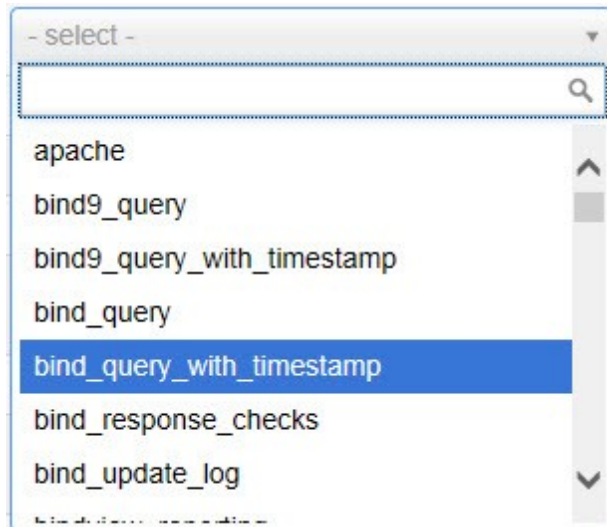


The screenshot shows the 'SNMP Distribution' page with the 'Add' button clicked. The table is empty, and the 'Save', 'Cancel', and 'Delete' buttons are visible.

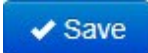
Distribution	Indexers

Buttons: Save, Cancel, Delete

3. Click inside the **Distribution** field and enter the name of a SNMP distribution inside the field. This is a suggest drop-down. Here you can select an existing distribution name (this means adding a new path to an existing distribution) or create a new one.
4. Enter a path in the **Path** field.
5. Click inside the Indexers field and from the drop-down select one or more indexers. You can search for an indexer by entering characters or words of the name of the indexer in the empty field located on drop of the drop-down list. To remove an indexer click the "X" of the name of the indexer.



**Note:** Indexers are optional, if none is entered only raw log files are stored on server.

7. Click . The new distribution is added to the list of distributions in the table.

### To modify a SNMP distribution

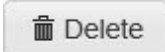
1. Double-click an editable field of a record in the table and it is enabled for editing. In the example the path field of a record has been double-clicked.



2. Edit the field as required.

3. Click  to save the changes. Click  to close without saving any changes made.

### To delete a SNMP distribution

1. Click to select the record of a SNMP distribution to be deleted.
2. Click . The delete confirmation dialog is displayed.



3. Click **Yes** to delete the record.

**Caution:** Exercise this function with care. The process cannot be undone. All data is deleted.



**Part**



**Managing  
Settings**

## 8 Managing Settings

In this chapter the various parameters and settings are discussed.

**Note:** Setting variables are system defined. They cannot be created via the application.

### To access the settings

1. Select **Settings** from the **Configuration** menu. The following page is displayed.

Name	Value
AD Accounts Location	-
AD admin password	-
AD admin username	-
AD Base DN	-
AD Server	-
AD Server Port	-
AD Username Field	-
data retention total usage warning limit (%)	75
notification email smtp host	localhost
security AD enabled	<input type="checkbox"/> OFF

Showing 1 to 10 of 14 entries

First Previous 1 2 Next Last

**Note:** These are the settings that will be visible/editable by users (with special roles):

The table below summarizes the behavior of each of the parameter variables.

Settings Variable	Property
AD Accounts Location	Specifies AD Account's location
AD admin password	Entry for the AD Administrator's password
AD admin username	Entry for the AD Admin's username
AD Base DN	Specifies Base DN (Distinguished name)
AD Server	Name of the AD Server
AD Server Port	Specifies AD Server Port
AD Username Field	Specifies the Username field
data retention total warning limit (%)	The capacity of a storage that when passed will cause the system to start sending out warning notifications. Also older files 30 days older are deleted allowing space for newer files. Expressed as a percentage.

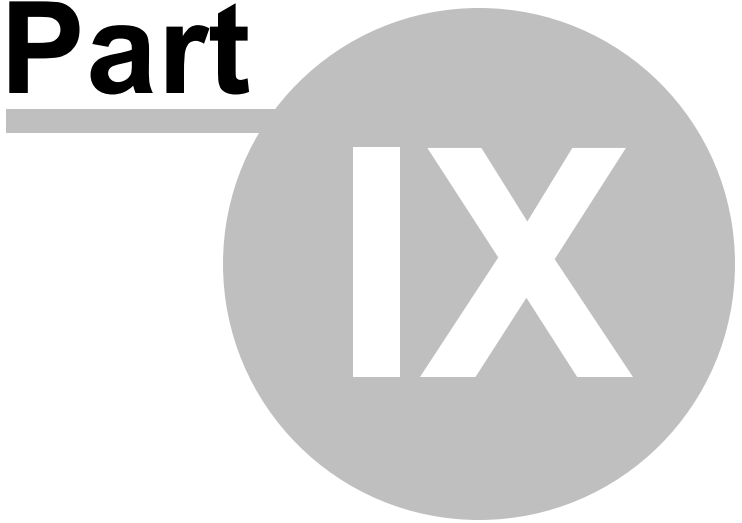


notification email SMTP host	The service that sends notification emails or alerts to the user or recipient.
security AD enabled	Enables/disables AD authorization. If enabled users are authenticated over AD before falling back to local database.
web export async row limit	Determines the maximum number of rows a table can have for it to be exported synchronously. The alternative is asynchronous download, which consists of emailing a user a download link once it is read.
web export async size limit (mb)	Determines the maximum total size files for them to be exported synchronously. The alternative is asynchronous download, which consists of emailing a user a download link once it is read.
web log viewer parse limit (mb)	Maximum size of logs to parse while doing a log raw search
web request_limit per user	Maximum concurrent "heavy" request per user (requiring many resources, file parsing, searching etc.,)

2. Double click the value field to modify the property of a setting variable if it is a value.



**Part**



**Creating and  
Managing  
Storage**

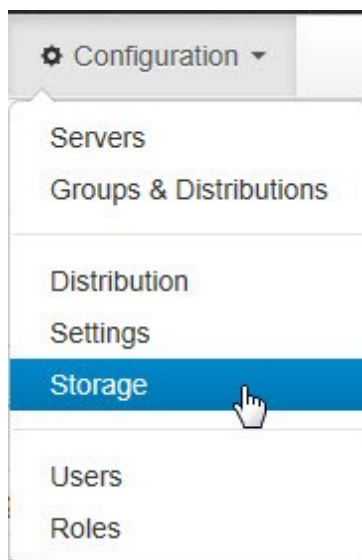
## 9 Creating and Managing Storage

These storage that are defined are the local storage on the central **OTUS** node, where the data that enters the system (copy methods) is stored. Your valuable data logs can then be archived and analyzed later. Using **OTUS SIEM** you can also create your own storage rule.

**Note:** The default storage is `/var/log/otus/storage1` and that it can't be deleted. However the path and size of this storage can be changed.

### To create or assign a storage space

1. Select **Storage** from the **Configuration** menu.



The web-page refreshes to display the following details.

Storage [Storage rule](#)

10  + Add

Name	Path	Size	Usage
store1	/var/log/otus/storage1	10 GB	<div style="width: 100%; height: 10px; background-color: green;"></div>
store2	/var/log/otus/storage2	4 GB	<div style="width: 100%; height: 10px; background-color: green;"></div>
store3	/var/log/otus/storage3	1 GB	<div style="width: 10%; height: 10px; background-color: green;"></div>
store4	/var/log/otus/storage4	1.10 GB	<div style="width: 27.85%; height: 10px; background-color: green;"></div>
store5	/var/log/otus/storage5	38.61 MB	<div style="width: 0%; height: 10px; background-color: green;"></div>


Showing 1 to 5 of 5 entries

First Previous 1 Next Last

**Note:** Positioning your mouse over the Usage graph or any record displays the actual storage space



used.

- Click . The following fields and buttons are displayed.



Name	Path	Size	Usage
		eg: 10 MB, 1	

- Click inside the box below **Name**. The box is enabled.
- Enter a name for the storage.
- Click inside the box below **Path**. The box is enabled.
- Enter the path (physical location) where the storage is to be located.
- Click inside the box below **Size**. The box is enabled.
- Enter the storage space of the storage in this box.

**Note:** The variable **data retention total warning limit (%)** under **Configuration -> Settings** determines when (at what limit of the storage space) notification is to be sent to the user.

- Click .

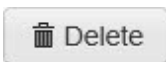
**Note:** In the initial state there is 1 default storage and 1 default storage rule (which points all incoming data to that default storage. It is of lowest priority.

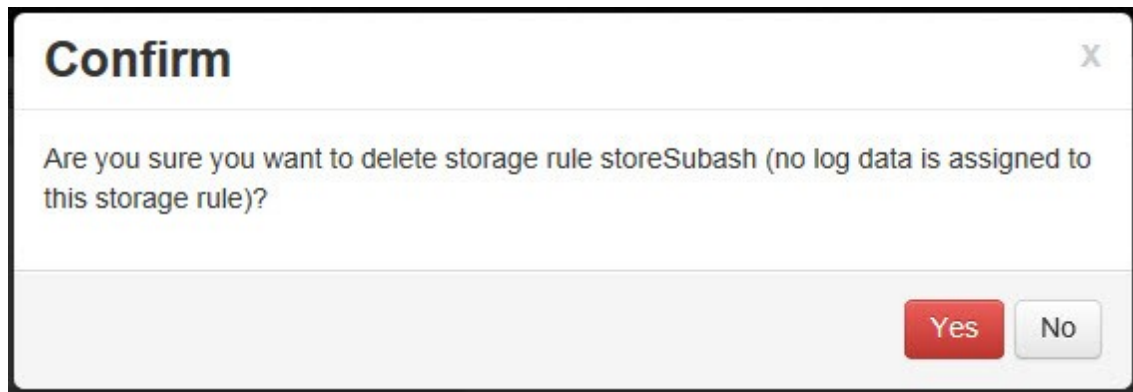
### To delete a storage

**Note:** You cannot delete a storage until you delete the storage rule associated with it

- From the list of storage records displayed select the one you wish to delete. It is highlighted as shown below.

storeSubash	/var/log/otus/storageSubash	10 MB	
-------------	-----------------------------	-------	--

- Click . The following delete confirmation dialog is displayed.



3. Click **Yes**.

**Caution:** Delete storage spaces with caution. The process is irreversible. When deleting a storage all its storage rules are also deleted. Affected log data is moved to new storages depending on the remaining storage rules.

#### To modify a storage

1. Double-click the **Name**, **Path** or **Size** fields of a record you wish to modify. The field is enabled for editing.
2. Edit the field as per your requirement.

3. Click  to save the changes or click  to cancel and close without saving any changes you have made.

## 9.1 Creating and Managing Storage Rules

Storage rules basically define which of your data, log files etc., goes where and when. For instance you would want your last year's data to be moved to a more archival area than your current year's data.

The following functions are also to be noted:

- when data enters the system it has to be assigned a storage rule, so the system knows on which storage to store it
- the system attempts to match all storage rules by priority, the first rule that is matched is used
- the default system rule can't be deleted or edited and is of the lowest priority. This ensures that all data will be matched by at least 1 storage rule
- Also, the topmost storage is tried first and when a match is encountered that match is used. If nothing matches, the default rule is used

#### To view the existing storage rules in the system

1. Click the **Storage** rule tab. The web page displays the following rules.

Storage Storage rule

Search:


+ Add Delete

Name	Servers	Groups	From	To	Storage	Retention	Priority
storage_itl44	itl442.info-sol.net	-	-	-	store3	365 days	↑ ↓
storage_imail	-	g_imail.g_nginx	-	-	store1	auto	↑ ↓
storage_powermta	-	g_powermta	-	-	store2	-	↑ ↓
default_storage_rule	-	-	-	-	store1	auto	↑ ↓

Showing 1 to 4 of 4 entries

**Note:** The **default\_storage\_rule** is a built-in-fallback rule that cannot be deleted and therefore it is disabled.

**To add a storage rule**

1. Click . Additional fields and buttons are displayed as shown below.

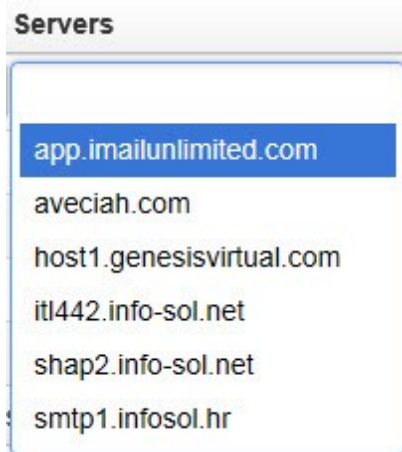
Storage Storage rule

Search:

Save Cancel Delete

Name	Servers	Groups	From	To	Storage	Retention	Priority
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	- select -	auto,n days,x %	↑ ↓

2. Enter a name for the storage rule in the box below **Name**.
3. Click inside the box below **Servers** and select 0 or more servers. The rule will match if the incoming data is from a server that is in this list of servers. The rule will also match if the list of servers is empty.



**Note:** You can select one or Groups servers for your storage. To remove a server from the box, click the "X" symbol of the server.

4. Click inside the box below **Groups** to select 0 or more groups. The rule will match if the incoming data is from a server in a group that is in this list of groups. The rule will also match if the list of groups is empty.

5. Click inside the box below **From/To** to add a start date when you want the storage rule to be in effect. The rule will match if the incoming data time is after/before the from/to datetime. The rule will match all data if from/to datetime is not defined.

6. Click inside the box below **To** to add an end date when you want the storage rule to end.

**Note:** How to use the calendar box and controls to select a date have been explained in the topic [Filtering Data using Filters](#) [22].

7. Select the storage that should be used to store data that matches this storage rule from the **Storage** drop-down list.

8. Enter the retention policy for data that matches this rule period in the box under **Retention**.

**Note:** There are three formats for entering the retention period. 1. **auto** - Where storage is filled to 100% and then the oldest files are deleted leaving only the newer ones. If this field is left empty then "auto" is automatically applied. 2. **n days** - Where files older than n days are deleted. 3. **X %** - Same as auto, but this storage rule is assigned % portion of the storage space.



9. Click .

**Note:** Also, the topmost storage is tried first and when a match is encountered that match is used. If nothing matches, the default rule is used

### To modify a storage rule

1. Double-click the field that needs to be modified and the field is enabled for editing as shown below. In the example below the **Name** field of a storage rule was double-clicked.



2. Modify the field and click  to save the changes. Click  to quit without saving the changes.

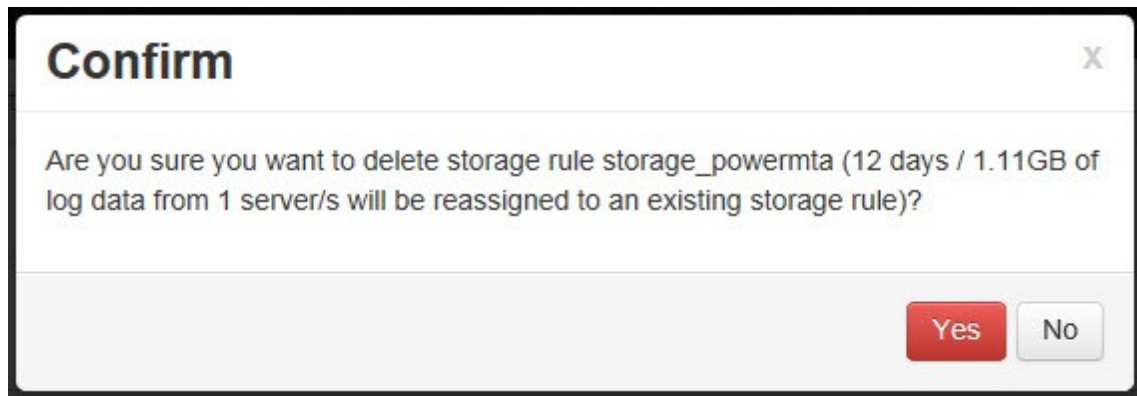
### To delete a storage rule

1. From the list of storage rules displayed select the storage rule you wish to delete. The selected storage rule is highlighted.



2. Click . The delete confirmation dialog is displayed.



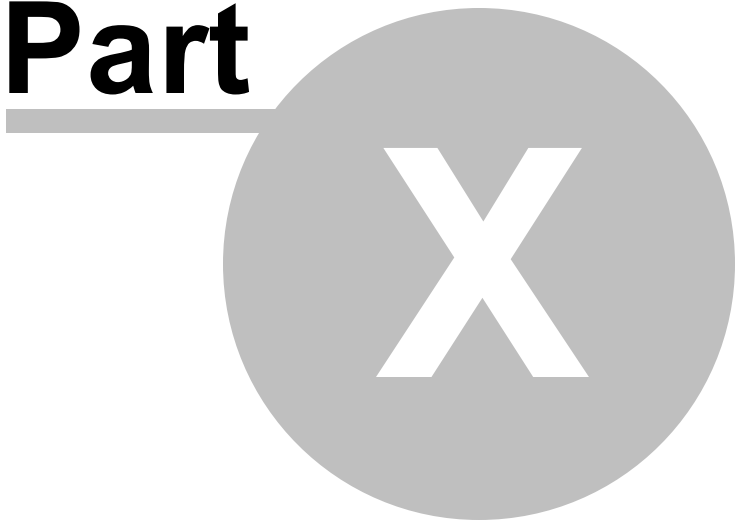


3. Click **Yes**.

**Caution:** Exercise this function with care. The process cannot be undone. Data stored using the rule is reassigned to another existing storage rule.



# Part



**User and Role  
Management**

## 10 User and Role Management

**OTUS SIEM** allows an administrator to create Role Based Access (RBAC) so that users can be restricted to accessing the system. Restrictions can be made such that a user can only view a particular part of the data and on a particular server and only for a particular date range. You can also restrict users to modules such that a user can only access a particular component such as indexing, configuration, alerting etc.,

### 10.1 Creating and Managing Users

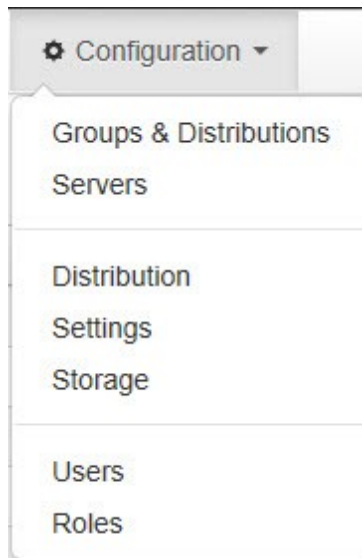
This topic explains how to add new users to the system. It also explains how to delete users.

**Note:** Only users with the **user\_config** role assigned to their profile can perform these functions. The **user\_config\_self** role permits changing user info (username, password) but not roles for themselves (i.e for the logged-in user). By default, every user has this role.

#### To create a user

1. Select **Users** from the **Configuration** menu.

**Note:** The follow menu appears for Admin/Root users only. Other users may have access to the Users menu but may not have complete functionality to create or edit users.



The web page refreshes to display the following screen. Notice that existing users of the system are displayed.

10

Username	Password	First name	Last name	Email	Roles
achandran81@gmail.com	-	Arun	Chandran	achandran81@gmail.com	always,config,demo,user_config_self
carviort@gmail.com	-	Carlos	Villaruel	carviort@gmail.com	always,config,user_config_self
debarghoghosh86@gmail.com	-	Debargho	Ghosh	debarghoghosh86@gmail.com	always,config,demo,user_config_self
delisaster@delisaster.com	-	Delisa	Simonovic	delisaster@delisaster.com	always,config,demo,user_config_self
denis@rpeer.com	-	Denis	Nuja	denis@rpeer.com	always,config,demo,user_config_self
djurica@infosol.hr	-	Damir	Jurica	djurica@infosol.hr	always,config,role-djurica@infosol.hr-G0EJH5pXkX2.role-djurica@infosol.hr-FLIOPdQc0W.role-djurica@infosol.hr
dsaric@itlab.hr	-	Dean	Saric	dsaric@itlab.hr	always,config,demo,user_config_self
dzadravec@gmail.com	-	Dominik	Z	dzadravec@gmail.com	always,config,demo,user_config_self
haicao8@gmail.com	-	Charles	Roy	haicao8@gmail.com	always,config,config_advanced,demo,user_config_self
itogola@msn.com	-	Ismaila	Togola	itogola@msn.com	always,config,demo,user_config_self

Showing 1 to 10 of 30 entries

**Note:** Using the **Search**   field you can also search for users. Just enter a few characters of the user's name and the page will filter records specific to your input characters or words.

2. Click . The web page displays the following additional fields and buttons.

10

Username	Password	First name	Last name	Email	Roles
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

3. Enter a username for the user in the **Username** field.

4. Enter a password in the **Password** field.

5. Enter the first name of the user in the **First name** field.

6. Enter the last name of the user in the **Last name** field.

7. Enter a valid e-mail id of the user in the **Email** field.

**Note:** This field is used for alerting the user and for asynchronous exports.

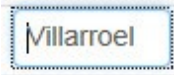
8. Click the **Roles** box and from the drop-down list select one or more roles.



**Note:** You can select multiple roles from the list. You may deleted a selected user by clicking the "X" symbol of the button. For more information on Roles please refer the topic [Creating and Managing Roles](#) <sup>102</sup>.

9. Click  to save the record.

### To modify a user

1. Double-click the field that needs to be modified and the field is enabled for editing as shown below. In the example below the **Last name** field of a user was double-clicked.



2. Modify the field and click  to save the changes. Click  to quit without saving the changes.

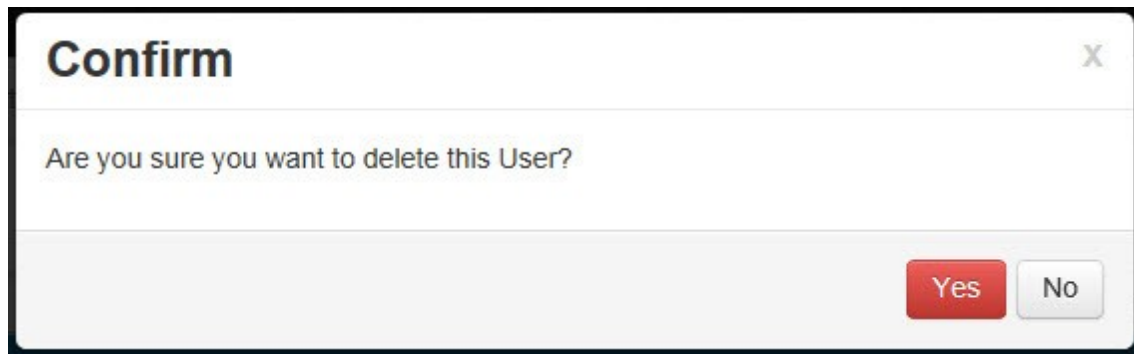
**Note:** When AD authentication is used password change doesn't have effect

### To delete a user

1. From the list of users displayed (refer step 1 of the previous section) select the user you wish to delete. The selected user is highlighted as shown below.



2. Click . The delete confirmation dialog is displayed.



3. Click **Yes**.

**Caution:** Exercise this function with care. The process cannot be undone. All data is deleted.

## 10.2 Creating and Managing Roles

Like employees in a company, users of OTUS, SIEM have roles. This topic explains how to create and manage roles. There are basically three types of roles. 1. Built-in roles, 2. Access Roles and 3. View Roles. The table below summarizes the responsibilities of each of them.

Role - Type	Function	Examples
Built-In Roles	Define what actions users are permitted to perform in the application. Cannot be created or deleted. They are built-in.	<b>config</b> - allows simple configuration of servers, groups and distribution.

		<p><b>config advanced</b> - permits advanced configuration functions such as configuring distribution, storage, settings</p> <p><b>user_config</b> - permits administration of users/roles</p> <p><b>user_config_self</b> - permits changing user info (username, password) but not roles for themselves (i.e for the logged-in user) Everyone by default has this role.</p> <p><b>superuser</b> - Can perform any or all the functions of the application.</p> <p><b>report</b> - A special function that permits a read-only view of all data and no configuration capability</p>
Access Roles	Define the time periods, a logged-in user can access the application. Users with the <b>user_config</b> role can create Access Roles.	<p><b>always</b> - users can access the system anytime</p> <p><b>working_hours</b> - users can access the application only during working hours of the company</p>
View Roles	Define what data a user can view on the application. Users with the <b>user_config</b> role can create View Roles.	

**Note:** The **Roles** option in the **Configuration** menu is displayed only for Superusers or users with the **user\_config** role.

This topic discusses the creation and managing of the various types of roles.

To manage the roles click **Roles** from the **Configuration** menu.



The following page is displayed

Access roles [View roles](#)

10


Name	Access
always	* 00:00-24:00
working_hours	mon-fri 08:00-18:00

Showing 1 to 2 of 2 entries

1


Click the **View roles** tab to view the other roles such as built-in roles.

### To create an access role

1. Click  on the **Access roles** page. The web page displays additional fields as shown below.

10

Name	Access
<input type="text"/>	<input type="text"/>
always	* 00:00-24:00
working_hours	mon-fri 08:00-18:00

2. Enter a name for the new access role in the **Name** box.
3. Enter a time period (use the existing time formats as a hint) in the **Access** box.
4. Click .

### To modify an access role

1. Double-click the field that needs to be modified and the field is enabled for editing as shown below. In the example below the Access field of an access role was double-clicked.

01:00-13:00

2. Modify the field as per your requirement.

**Note:** A few correct formats are **mon-sat 09:00-09:30**, **09:00-10:00**, **mon-fri 09:00-09:30**, **10:00-13:30** etc.,

3. Click  to save the changes. Click  to quit without saving the changes.

### To delete an access role

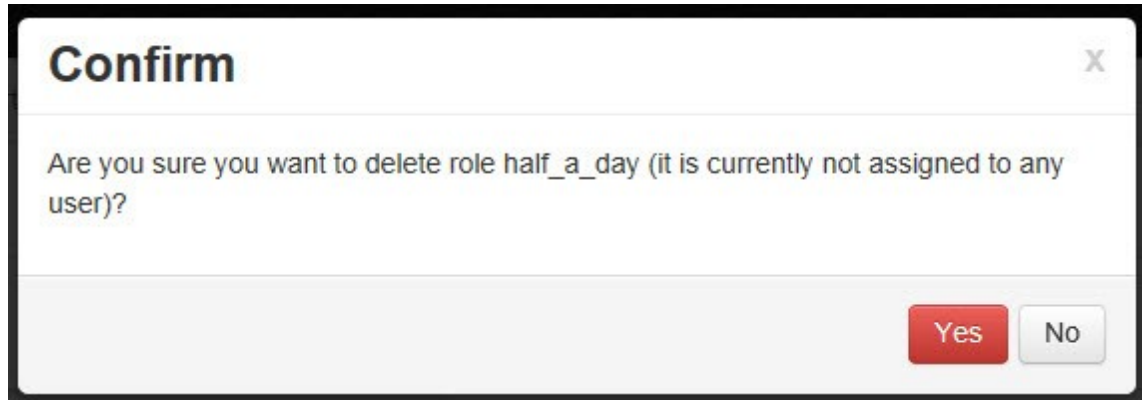
1. Select an access role from the list. It is highlighted by a blue background as shown below.



half\_a\_day

mon-fri 09:00-12:00

2. Click .



3. Click **Yes** to delete or click **No** to abort the operation.

**Caution:** Exercise this function with care. The process cannot be undone. All data is deleted.


### To create a view role

Ensure you are at the **View Roles** page as shown below.

Access roles View roles

10

Name	Servers	Groups	From	To
demo	aveciah.com,host1.genesisvirtual.com,smtp1.infosol.hr	-	-	-
role-djurica@infosol.hr-fLIOPdQc0W	smtp1.infosol.hr	-	-	-
role-djurica@infosol.hr-G0EJH5pXKX2	-	g_email	-	-
role_djurica@infosol.hr_g_new	-	g_new	-	-
role_djurica@infosol.hr_g_nginx	-	g_nginx	-	-
role_djurica@infosol.hr_g_powermta	-	g_powermta	-	-
role_djurica@infosol.hr_s_app.imailunlimited.com	app.imailunlimited.com	-	-	-
role_djurica@infosol.hr_s_itl442.info-sol.net	itl442.info-sol.net	-	-	-
role_djurica@infosol.hr_s_lueshari.org2	-	-	-	-
role_g_nginx	-	g_nginx	-	-

1. Click . The following fields and buttons are displayed.

Access roles View roles

10

Name	Servers	Groups	From	To
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

2. Enter the name of a role in the **Name** box.

- Click inside the **Servers** box to choose one or more servers from the drop-down list.

**Note:** Users assigned this role can view data originating only from these server. You can search for servers by typing the first few characters of the server name. To delete a server from the **Servers** box, click the "X" symbol of the server.

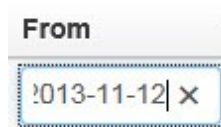
- Click inside the **Groups** box to choose one or more groups from the drop-down list.

**Note:** Users assigned this role can view data originating only from servers that are assigned to these groups. You can search for groups by typing the first few characters of the group's name. To delete a server from the **Groups** box, click the "X" symbol of the group.



- Click inside the **From** box to invoke the calendar as shown below.



Use the calendar control to select a **From** date for the role. The role is in effect in the system from the **From** date onwards.

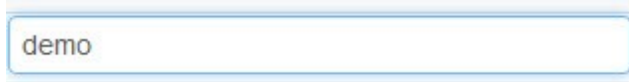




**Note:** Users assigned this role can view log data created only during this date/time range.

- Click . The new role is listed in the table displaying roles in the system. To quit without saving click .

**To modify a view role**

1. Double-click the field that needs to be modified and the field is enabled for editing as shown below. In the example below the **Name** field of a view role was double-clicked.



2. Modify the field and click  to save the changes. Click  to quit without saving the changes.

### To delete a view role

1. Select the view role to delete. The role is highlighted as shown below.



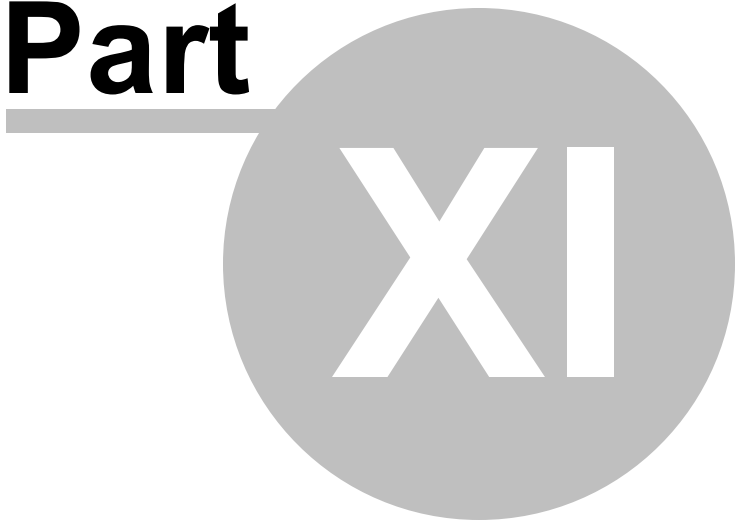
2. Click . The delete confirmation dialog is displayed.



3. Click **Yes** to delete. Click **No** to quit.



**Part**



**System**

## 11 System

This chapter discusses how to view system related information such as status and events related to the system. This menu is displayed only the System Administrator or Superuser.

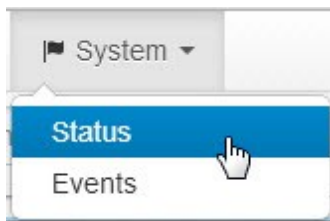
**Note:** The role **Superuser** if assigned to a user will enable the **System** menu on his or her dashboard.

### 11.1 System > Viewing system status

This option gives the logged in user a complete status of the system. The information displayed is restricted to the type of user logged in. The following is for the Administrator (Super User) of the system.

#### To view system status

1. Select **Status** from the **System** menu.



The following page is displayed.

 A screenshot of the 'System Status' page. It is divided into four main sections:
 

- Service status:** A list of services with their status (running). Services include: celery, celery alert, celery beat, celery clean, celery copy, celery es, celery index, celery index group, celery organize, celery schedule, push snmp listener, push syslog listener, and rpc server.
- Modules:** A list of modules with their status (running). Modules include: alerting (distributed realtime reporting), indexing (SQL like search functions), reporting (processed records), snmp (snmp listener), storage (multiple storage rules), syslog (sdlog listener), and users (role based access (RBAC)).
- License:** Shows 'static license' for 'User 7' with a note 'This license never expires'.
- Server info:** A table showing host details: Host Name (snms-InfoSec-04), Host Address (10.10.10.110), and Host Load (3.30 4.70 6.43).

**Note:** **Services** are those processes that are running in the background. These should always be running. **Modules** refer to application functionality and some of these can be disabled.

The following tables summarizes the functions of the various statuses.

#### Celery Global Scheduling Process

Status	Function
celery alert	alert scheduling process
celery beat	cron scheduling process

celery copy	PULL fetching process
celery index	indexer worker process
celery index group	indexer group worker process
celery organize	path storage process
celery schedule	cron scheduling process

### Others

Status	Function
push snmp listener	snmp listener process
push syslog listener	syslog listener process
rpc server	RPC listener process
alerting	alerting menu tab
indexing	indexing menu tab
reporting	reporting menu tab
snmp	snmp listener functionality
storage	multiple storage rules functionality
syslog	syslog listener functionality
users	Role base access (RBAC) functionality
static licence	checks if licence is valid

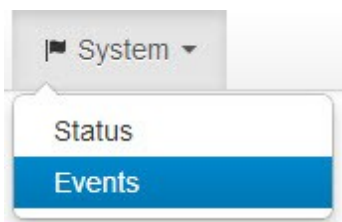
## 11.2 System > Viewing system events

This option allows you to view events related to the system.

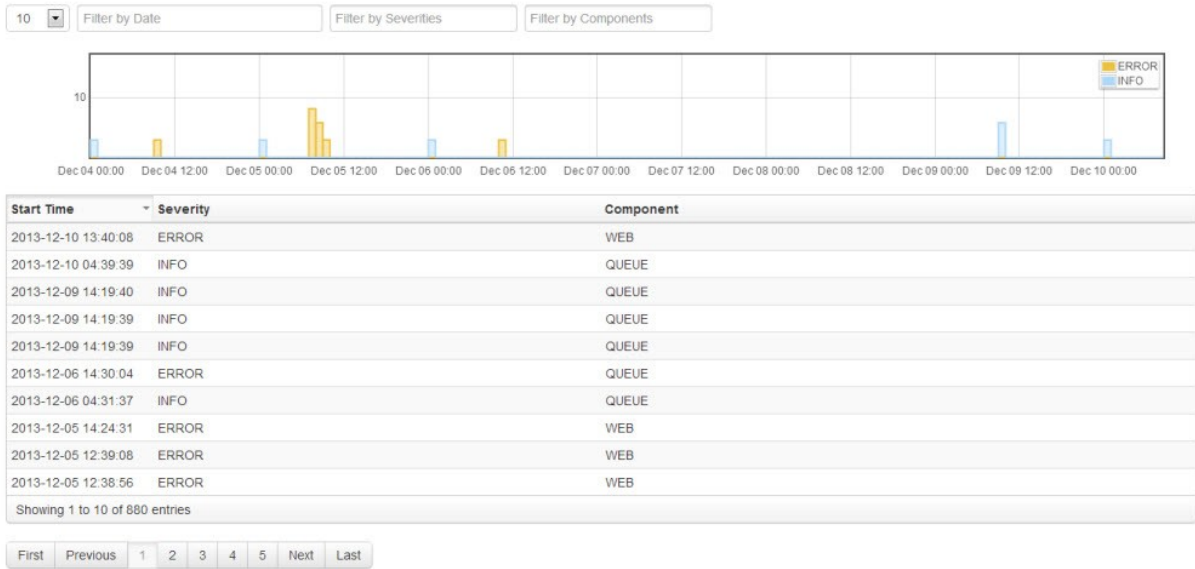
**Note:** This screen is for debugging purposes only and is enabled only for users with the superuser role.

### To view system events

1. Select **Events** from the **System** menu.



The following page about the events of the system is displayed.



2. Filter the data using one or more filters. Refer the [Filtering data using filters](#)<sup>[22]</sup> topic for more information on how to use filters. The Graph also displays information and the ways to use the Graph has been detailed in the topic [Instant Graph](#)<sup>[20]</sup>.

3. Click a record for more detailed information. Below is the image of a INFO record, when selected.

2013-12-10 04:39:39 INFO QUEUE

**event:**

```
single retent
```

**path:**

```
/var/log/otus/storage3/g_nginx/it1442.info-sol.net/NginxDistro/var$log$nginx$brojac.itlab.hr-access.log*/2013/09/10.log
```

Below is the image of a ERROR record selected. Details of the trace captured is displayed.



```

2013-12-06 14:30:04 ERROR QUEUE
trace:
Traceback (most recent call last):
  File "/usr/local/lib/python2.7/dist-packages/celery/task/trace.py", line 233, in trace_task
    R = retval = fun(*args, **kwargs)
  File "/usr/local/lib/python2.7/dist-packages/celery/task/trace.py", line 420, in __protected_call__
    return self.run(*args, **kwargs)
  File "/svn/otus/backend/otus/tasks/generictask.py", line 44, in run
    self.work(*args,**kwargs)
  File "/svn/otus/backend/otus/tasks/async/copy.py", line 56, in work
    job.copystatus = constants.job.copystatus.COMPLETED
  File "/svn/otus/backend/otus/db/transactions.py", line 37, in __exit__
    self.sessionobj.commit()
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/orm/session.py", line 656, in commit
    self.transaction.commit()
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/orm/session.py", line 314, in commit
    self._prepare_impl()
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/orm/session.py", line 298, in _prepare_impl
    self.session.flush()
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/orm/session.py", line 1583, in flush
    self._flush(objects)
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/orm/session.py", line 1654, in _flush
    flush_context.execute()
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/orm/unitofwork.py", line 331, in execute
    rec.execute(self)
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/orm/unitofwork.py", line 475, in execute
    uow
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/orm/persistence.py", line 59, in save_obj
    mapper, table, update)
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/orm/persistence.py", line 485, in _emit_update_statements
    execute(statement, params)
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/engine/base.py", line 1449, in execute
    params)
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/engine/base.py", line 1584, in _execute_clauseelement
    compiled_sql, distilled_params
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/engine/base.py", line 1698, in _execute_context
    context)
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/engine/base.py", line 1691, in _execute_context
    context)
  File "/usr/lib/python2.7/dist-packages/sqlalchemy/engine/default.py", line 331, in do_execute
    cursor.execute(statement, parameters)
IntegrityError: (IntegrityError) duplicate key value violates unique constraint "remote_log_file_md5_server_id_pulldistributiongrouppulldata_idx"
DETAIL:  Key (md5, server_id, pulldistributiongrouppulldatatype_id, filename)=(d41d8cd98f00b204e9800998ecf8427e, 13, 14, /var/log/nginx/trac.info-sol.net-access.log) already exists.
"UPDATE remote_log_file SET job_id=%(job_id)s, filename=%(filename)s, atime=%(atime)s, mtime=%(mtime)s WHERE remote_log_file.id = %(remote_log_file_id)s" {'mtime': datetime.datetime(2013, 12, 6, 9, 52, 21), 'atime': datetime.datetime(2013, 12, 6, 9, 52, 59), 'remote_log_file_id': 2447, 'job_id': 141257, 'filename': 'u'/var/log/nginx/trac.info-sol.net-access.log'}
}

task:
otus.tasks.async.copy.CopyTask

task_kwargs:
{}

task_id:
copy_job_#141257

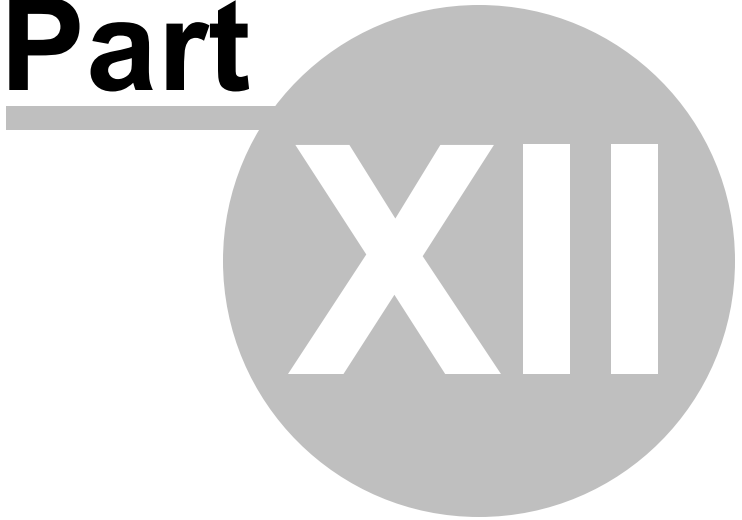
pid:
22270

task_args:
(141257, 'SCP')

```



**Part**



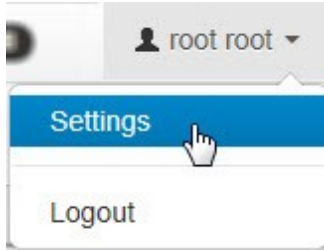
**Logged in User  
Settings**

## 12 Logged in User Settings

These are settings exclusive to the user that has logged in.

### To view the settings of the logged in user

1. Select Settings from the user menu as shown in the image below.



The web page displays the following information.

Name	Value
log content dateformat	%b %d %H:%M:%S
notification web notify alert	<input checked="" type="checkbox"/> ON
notification web notify job success	<input checked="" type="checkbox"/> ON
notification web notify push success	<input checked="" type="checkbox"/> ON
web log analysis reduce	<input checked="" type="checkbox"/> ON
web log raw reduce	<input checked="" type="checkbox"/> ON
web search regex case sensitive	<input type="checkbox"/> OFF

Showing 1 to 7 of 7 entries


First Previous 1 Next Last

The table below summarizes the behavior of each of the parameter variables.

Settings Variable	Property
log content dateformat	<p>The default time format to use when displaying raw log data. If left empty the system will use the original time format which was used to store the incoming data locally</p> <p><b>Note:</b> For a list of OTUS time formats please refer the topic <a href="#">List of OTUS time formats</a><sup>120</sup>.</p>
notification web notify alert	Sets notification for alerts should notifications for alert events be visible.

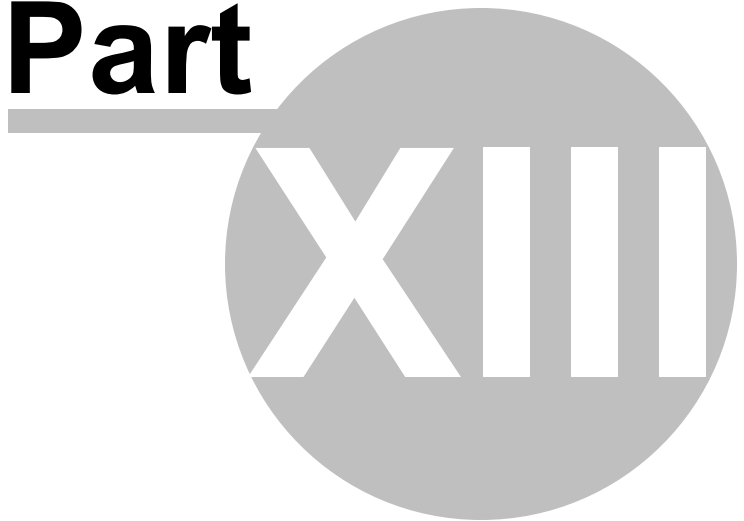
notification web notify job success	Sets notifications for successful jobs should notification for pull copy success be visible.
notificaiton web notify push success	Sets notifications for successful data push jobs should notifications for push copy success be visible.
web log analysis reduce	When enabled the system will cascade equivalent indexed rows (adjacent & close in time) and show only 1 row with a multiple marker on the side (example browser js console errors).
web log raw reduce	Same as above, but this setting concerns raw log rows. Also if it is on it will join similar lines together in one row and put a marker with a name if similar rows exist before that row. Works for log viewer for raw log files.
web search regex case sensitive	To enable or disable case sensitive search when searching regex in raw logs.

2. Double click the value field to adjust or modify the property of a setting variable if it is a value. If it is a

**ON/OFF**  toggle button then click once to change its value.



**Part**



**List of OTUS time  
formats**

## 13 List of OTUS time formats

This is a chart of the various OTUS time formats.

Directive	Meaning
%a	Locale's abbreviated weekday name.
%A	Locale's full weekday name.
%b	Locale's abbreviated month name.
%B	Locale's full month name.
%C	Common Log Format (CLF) ex: [10/Oct/2000:13:55:36 -0700]
%d	Day of the month as a decimal number [01,31].
%H	Hour (24-hour clock) as a decimal number [00,23].
%I	Hour (12-hour clock) as a decimal number [01,12].
%j	Day of the year as a decimal number [001,366].
%m	Month as a decimal number [01,12].
%M	Minute as a decimal number [00,59].
%p	Locale's equivalent of either AM or PM.
%S	Second as a decimal number [00,61].
%t	Unix time, the number of seconds since 00:00:00 UTC on January 1, 1970
%T	TAI 64 time format
%U	Week number of the year (Sunday as the first day of the week) as a decimal number [00,53]. All days in a new year preceding the first Sunday are considered to be in week 0.
%w	Weekday as a decimal number [0(Sunday),6].
%W	Week number of the year (Monday as the first day of the week) as a decimal number [00,53]. All days in a new year preceding the first Monday are considered to be in week 0.
%y	Year without century as a decimal number [00,99].
%Y	Year with century as a decimal number.
%%	A literal '%' character.



# Index

## - A -

- adding a user 100
- alert 38
- alert queries 38
- alert rules 43
- alerting 38
- alerts 38
- auto-detection 70

## - C -

- configuration 70
- creating a report 61
- creating alert rules 43
- creating alerts 38
- creating and managing servers 70
- creating and managing storage rules 94
- creating distributions 75
- creating groups 73
- creating PULL distribution 76
- creating reports 56
- creating roles 102
- creating rule instances 48
- creating SNMP distribution 83
- creating storage 92
- creating storage rule 92
- creating SYSLOG distribution 79
- creating users 100
- creating account 12
- customizing a report 66

## - D -

- data downloading 32
- deleting a report 61
- deleting alerts 38
- deleting distributions 75
- deleting groups 73
- deleting roles 102
- deleting rule 43
- deleting rule instance 48
- deleting servers 70

- deleting SNMP distribution 83
- deleting storage 92
- deleting storage rule 92
- deleting SYSLOG distribution 79
- deleting users 100
- distribution 75, 76
- distributions 75
- downloading data 32

## - E -

- editing alert queries 38
- editing distributions 75
- editing groups 73
- editing roles 102
- editing servers 70
- editing users 100
- events 111

## - F -

- filtering data 22

## - G -

- gmail 7
- google account 7
- group 73
- groups 73

## - H -

- hardware 6
- help 6

## - I -

- index log 36
- index log search 36
- indexing 36
- indexing data 36
- instant graph 20
- introduction 6

**- L -**

license 110  
logged in user settings 116  
login 7  
logout 7  
lost password 7

**- M -**

managing alert queries 38  
managing alert rules 43  
managing PULL distribution 76  
managing settings 88  
modifying SNMP distribution 83  
modifying storage 92  
modifying storage rule 92  
modifying SYSLOG distribution 79  
modules 110

**- N -**

notifications 27

**- O -**

OTUS account 12  
OTUS SIEM 6

**- P -**

password 7  
password recovery 7  
PULL copy 70  
PULL distribution 76  
PUSH copy 70

**- R -**

raw data 32  
raw log search 16  
raw logs page 16  
raw logs search page 16  
raw logs searching 16  
RBAC 100

regex 22  
register 12  
registering 12  
regular expression 22  
report 61  
reporting 61  
reports 56, 66  
role 100, 102  
role based access 100  
roles 100, 102  
rule 48  
rule instances 48

**- S -**

server info 110  
servers 70  
service status 110  
settings 70, 88, 116  
SNMP 83  
SNMP distribution 83  
software 6  
storage 92  
storage rule 92, 94  
storage rules 92, 94  
SYSLOG 79  
SYSLOG distribution 79  
system events 111  
system requirements 6  
system status 110

**- T -**

text search 22  
time formats 120

**- U -**

user 100  
users 70, 100, 110  
using filters 22

**- V -**

viewing logs 32  
viewing data 32