

NG Trace
User Manual

December 2009

Table of Contents

1. INTRODUCTION.....	4
1.1 OVERVIEW	4
2. SYSTEM OVERVIEW.....	4
2.1 ABOUT THE SYSTEM.....	4
2.2 FEATURE	4
2.3 SYSTEM REQUIREMENT.....	4
3. USER MANAGEMENT.....	5
3.1 USER LOG IN	5
3.2 USER MANAGEMENT.....	6
3.3 USER PRIVILEGE	10
4. REPORT AND ANALYSIS.....	11
4.1 LOGS AND AUDITS	11
4.1.1 <i>Whole</i>	11
4.1.2 <i>ICMP</i>	14
4.1.3 <i>E-mail</i>	16
4.1.4 <i>IM</i>	19
4.1.5 <i>HTTP</i>	20
4.1.6 <i>FTP</i>	22
4.2 SEARCH.....	25
4.3 DATABASE	25
4.4 EXPORT	27

Table of Figures

FIGURE 1. USER LOG IN.....	5
FIGURE 2. USER MANAGEMENT TAB.....	6
FIGURE 3. ADD USER.....	7
FIGURE 4. SHOW USER INFORMATION.....	8
FIGURE 5. EDIT USER	9
FIGURE 6. SET NEW PASSWORD	10
FIGURE 7. WHOLE LOG LIST.....	12
FIGURE 8. RESULT FILTER OF WHOLE LOG LIST.....	12
FIGURE 9. DATE – TIME FILTER.....	13
FIGURE 10. PROTOCOL FILTER	13
FIGURE 11. TARGET FILTER.....	13
FIGURE 12. HOST FILTER.....	14
FIGURE 13. PAGE FILTER.....	14
FIGURE 14. ICMP LOG LIST	15
FIGURE 15. RESULT FILTER OF ICMP LOG	15
FIGURE 16. EXPORT MESSAGE.....	16
FIGURE 17. ICMP DETAIL	16
FIGURE 18. E-MAIL LOG LIST	17
FIGURE 19. RESULT FILTER OF E-MAIL LOG	17
FIGURE 20. EXPORT MESSAGE.....	18
FIGURE 21. E-MAIL DETAIL.....	18
FIGURE 22. IM LOG LIST	19
FIGURE 23. RESULT FILTER OF IM LOG	20
FIGURE 24. EXPORT MESSAGE.....	20
FIGURE 25. HTTP LOG LIST	21
FIGURE 26. RESULT FILTER OF HTTP LOG.....	21
FIGURE 27. EXPORT MESSAGE.....	22
FIGURE 28. HTTP DETAIL.....	22
FIGURE 29. FTP LOG LIST	23
FIGURE 30. RESULT FILTER OF FTP LOG	23
FIGURE 31. EXPORT MESSAGE.....	24
FIGURE 32. FTP DETAIL.....	24
FIGURE 33. SEARCH	25

FIGURE 34. SELECT DATABASE	26
FIGURE 35. WHOLE LOG LIST OF RECENTDB.....	27
FIGURE 36. EXPORT TABLE LIST	28

1. Introduction

1.1 Overview

This document describes information on the usage of the system from the user point of view.

It explains about the different user account and their privileges, the options for exporting the result as CSV file, using the different reports and analysis pages, searching and filtering the results.

2. System Overview

2.1 About the System

NG Trace is a corporate security which is capable of monitoring the network traffic and taking action on the occurrence of suspicious or potentially dangerous events.

NG Trace as any modern security system is with flexible, multi-layered and easily configurable architecture and software design.

It has intuitive user-friendly interface and lots of functionalities.

It can apply both set of predefined rules following suspicious users' behavior and it can accept new targets of interest defined by newly inserted rule sets.

2.2 Feature

- ✓ Capturing network traffic, transferring it to readable look and connecting of communication sessions.
- ✓ Saving the decoded traffic into database.
- ✓ Indexing of the decoded traffic into database.
- ✓ Exporting the data of database.
- ✓ Archiving of the database on hardware device.
- ✓ Sending e-mails in case of the emerging of difference event.

2.3 System Requirement

OS : Cent OS 5.3 recommended.

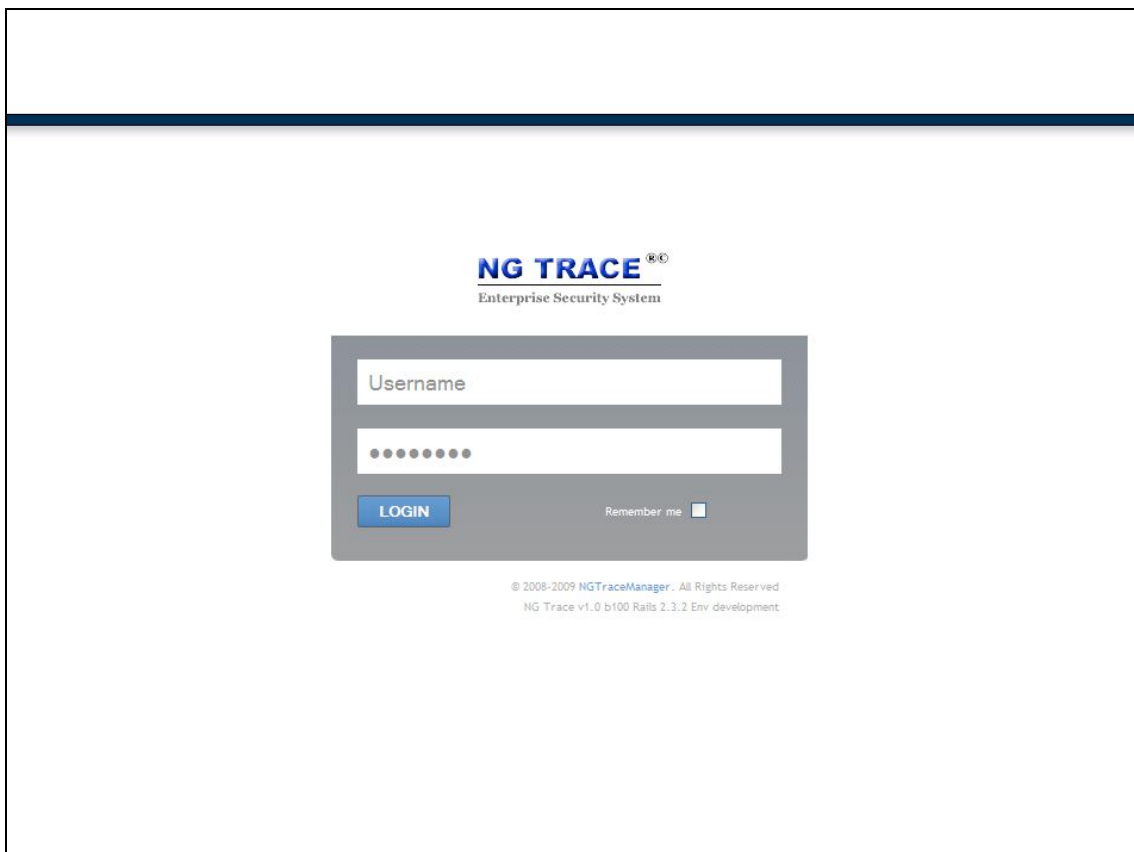
The system's components run on Intel based, GNU / Linux compatible server machines, equipped with at least one network card, a CD / DVD drive, enough hard-disk space and RAM.

If all the system's components are deployed on a single server;
Dual Core 2.4GHz Pentium CPU,
4GB RAM system memory,
80GB available disk space or more
100Mbit/s Network card or more

3. User Management

3.1 User Log In

User with user account enters Username and Password to log in.



The screenshot displays the login page for the NG TRACE Enterprise Security System. At the top center, the logo reads "NG TRACE" in blue, with a registered trademark symbol, and "Enterprise Security System" in smaller black text below it. The main login area is a gray-bordered box containing a "Username" input field, a password input field with masked dots, a blue "LOGIN" button, and a "Remember me" checkbox. At the bottom of the page, small text indicates the copyright: "© 2008-2009 NGTraceManager. All Rights Reserved" and the version: "NG Trace v1.0 b100 Ralls 2.3.2 Env development".

Figure 1. User Log In

3.2 User Management

User management section provides functionalities such as adding and deleting of user, displaying and modifying user's information.

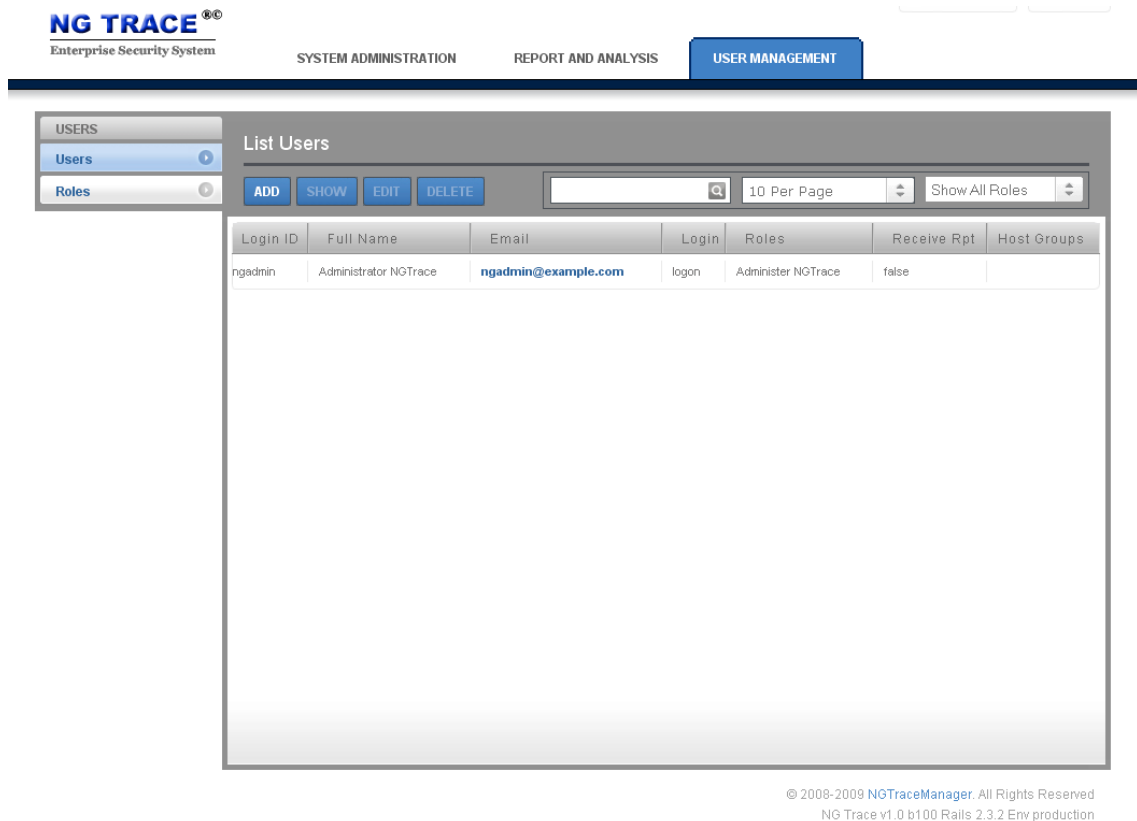


Figure 2. User Management Tab

User information contains user login ID, user name, e-mail address, phone number, registered date, modified date, option whether or not to receive notify information from notifier, login status, login date/time, user role, manageable host groups, description and etc.

- [ADD] :

Register new user.

Enter user information of new user.

Login ID and e-mail address should not be same as the ones of already registered users.

Symbol “*” indicates mandatory fields. If mandatory field is left blank, user registration is not processed.

If user role “Administer NG Trace” is selected, other user role options become disabled. “Groups” item becomes activated only if user role “Group Part Admin” or “Group Part Viewer” is selected.

The screenshot displays the NG TRACE Enterprise Security System interface. At the top, there is a navigation bar with the logo, system name, and tabs for SYSTEM ADMINISTRATION, REPORT AND ANALYSIS, and USER MANAGEMENT. The USER MANAGEMENT tab is active. On the left, a sidebar shows 'USERS' with sub-items 'Users' and 'Roles'. The main content area is titled 'New User' and contains a form with the following fields: Username, Email, First Name, Last Name, Phone Number, Report Receiver (a dropdown menu currently set to 'NO'), Password, Confirm Password, and Description. Below these fields is a 'Roles' section with a list of checkboxes: Administer NGTrace, Analyst Administrator, Analyst Viewer (which is checked), System Administrator, System Viewer, User Administrator, User Viewer, Group Part Admin, and Group Part Viewer. At the bottom of the form is a 'Groups' section with the text '(This user can manage host groups as below)' and two checkboxes for 'group 1' and 'group 2'. A 'SAVE' button is located at the bottom right of the form.

Figure 3. Add User

- [SHOW]

We can view selected User's information.

User's Information includes the Login ID, Name, Email Address, phone number, creation date/time, update date/time, Logon Status, Roles, Host Groups, and Description.

“Create at” indicates created time and “Update at” represents updated time.

Logon Status shows login state if user is login.

Roles field shows privilege of user.

The screenshot displays the NG TRACE Enterprise Security System interface. At the top, there is a navigation bar with the logo 'NG TRACE Enterprise Security System' on the left, and buttons for 'ngadmin' and 'Logout' on the right. Below the logo, there are three tabs: 'SYSTEM ADMINISTRATION', 'REPORT AND ANALYSIS', and 'USER MANAGEMENT', with 'USER MANAGEMENT' being the active tab.

On the left side of the main content area, there is a sidebar with a 'USERS' section containing 'Users' and 'Roles' links. The 'Users' link is selected, and a 'LIST ALL USERS' button is visible.

The main content area is titled 'Show User Information Of Ngadmin'. It contains a form with the following fields and values:

Login ID :	ngadmin
Name :	Administrator NGTrace
Email Address :	ngadmin@example.com
Phone Number :	0415235634433
Created at :	2009-08-15 02:42:38 UTC
Updated at :	2009-11-20 18:00:50 UTC
Report Receiver :	true
Logon Status :	Logon
Logon Time :	2009-11-20 18:00:50 UTC
Roles :	Administer NGTrace
Description	default administrator

At the bottom right of the page, there is a copyright notice: '© 2008-2009 NGTraceManager. All Rights Reserved' and 'NG Trace v1.0 b100 Rails 2.3.2 Env production'.

Figure 4. Show User Information

- **[EDIT]**

You can edit information and password of registered user here.

If user role “Administer NG Trace” is selected, other user role options become disabled. “Groups” item becomes activated only if user role “Group Part Admin” or “Group Part Viewer” is selected.

NG TRACE[®]

Enterprise Security System

SYSTEM ADMINISTRATIONREPORT AND ANALYSIS

USER MANAGEMENT

ngadminLogout

USERS

Users

Roles

Edit User 'Ngadmin'

LIST ALL USERS

CHANGE PASSWORD

Username

ngadmin

Email

ngadmin@example.com

First Name

Administrator

Last Name

NGTrace

Phone Number

0415235634433

Report Receiver

YES

Description

default administrator

Roles

☒ Administrator NGTrace

☐ Analyst Administrator

☐ Analyst Viewer

☐ System Administrator

☐ System Viewer

☐ User Administrator

☐ User Viewer

☐ Group Part Admin

☐ Group Part Viewer

Groups(This user can manage host groups as below)

☐ group 1

☐ group 2

SAVE

© 2008-2009 NGTrace Manager, All Rights Reserved

NG Trace v1.0 b100 Patch 2.3.2 Exp production

Figure 5. Edit User

To change the Password, input new Password and Confirm Password, press [SAVE].

The screenshot displays the NG TRACE Enterprise Security System interface. At the top, the logo 'NG TRACE' is visible, along with the text 'Enterprise Security System'. Navigation tabs include 'SYSTEM ADMINISTRATION', 'REPORT AND ANALYSIS', and 'USER MANAGEMENT'. A user profile 'ngadmin' with a 'Logout' button is in the top right. On the left, a sidebar shows 'USERS' with sub-items 'Users' and 'Roles'. The main content area is titled 'Set New Password' and contains two input fields: 'Password' and 'Confirm Password', followed by a 'SAVE' button. Below the form, a copyright notice reads: '© 2008-2009 NGTraceManager. All Rights Reserved. NG Trace v1.0 b100 Rails 2.3.2 Env development.'

Figure 6. Set New Password

- [DELETE]
You can delete selected User from user list.

3.3 User Privilege

NG Trace Management Console provides several user privileges such as Administer NGTrace, Analysis Administrator, Analysis Viewer, System Administrator, System, Viewer, User Administrator, User Viewer, Group Part Admin and Group Part Viewer.

- Administer NG Trace
The user of an account with Administer NG Trace privilege has all privilege of NG Trace System.
That is, can manage all information within SYSTEM ADMINISTRATION page and REPORT AND ANALYSIS page and USER MANAGEMENT.
- Analysis Administrator

The user with this privilege has access to all functionalities of REPORT AND ANALYSIS page.

- Analysis Viewer

The user with this privilege can only view information of REPORT AND ANALYSIS page.

- System Administrator

The user with this privilege has access to all functionalities of SYSTEM ADMINISTRATION page.

- System viewer

The user with this privilege can only view information of SYSTEM ADMINISTRATION page.

- User Administrator

The user with this privilege has access to all functionalities of USER MANAGEMENT page.

- User Viewer

The user with this privilege can only view information of USER MANAGEMENT page.

- Group Part Admin

- Group Part Viewer

4. Report and Analysis

4.1 Logs and Audits

4.1.1 Whole

Show list of stored Logs and audits in selected DB.

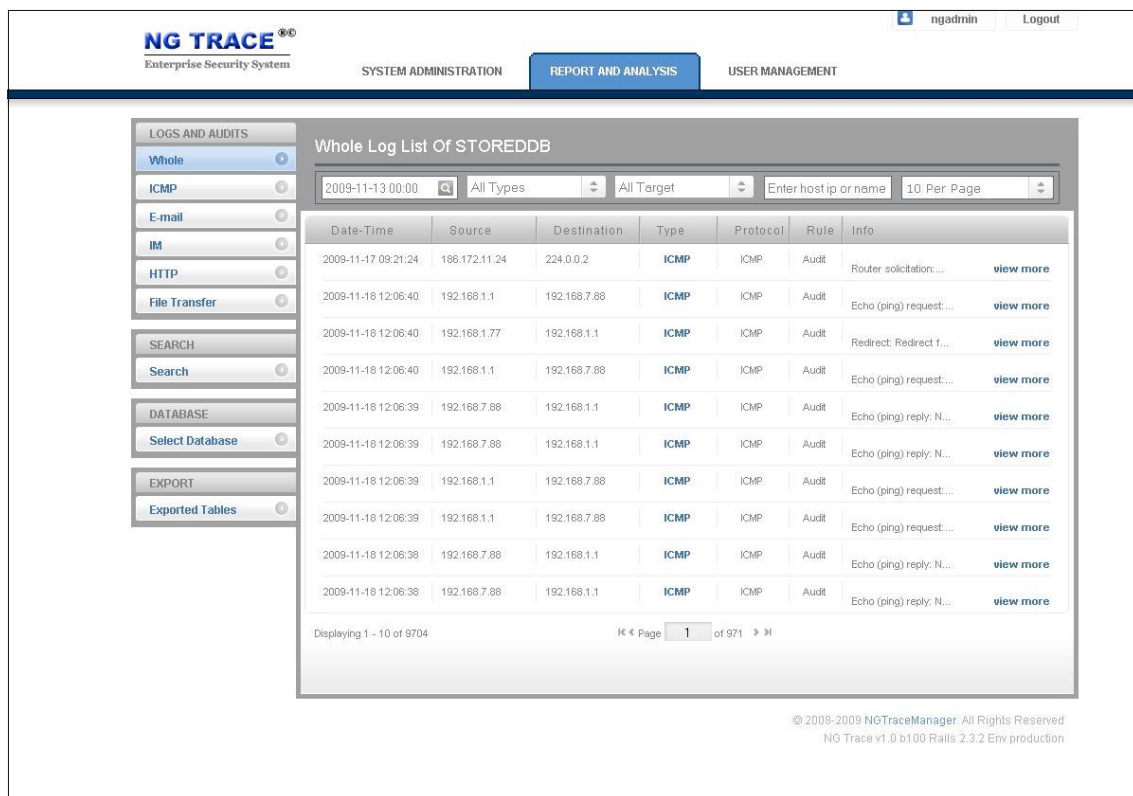


Figure 7. Whole Log List

The following information displays contents of recorded whole log.

- Date – Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Type: Type of communication protocol.
- Protocol: Type of sub protocol.
- Rule: Target information.
- Info: Summarize information of carried contents.
- [view more]: Can see detail information of carried contents.

User can filter Whole Log List by Date-Time, Protocol, Target, Host, and Page.



Figure 8. Result Filter of Whole Log List

- Date – Time Filter



Figure 9. Date – Time Filter

Filter whole Log List by date – time.

It shows all logs recorded since specified date/time to current date/time.

- Type filter

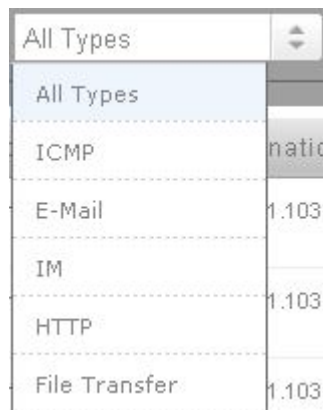


Figure 10. Protocol Filter

It allows filtering whole Log List by Protocol.

It shows searched result by selected protocol.

For example, if selected E-mail protocol, user can see only E-mail communication log.

- Target Filter

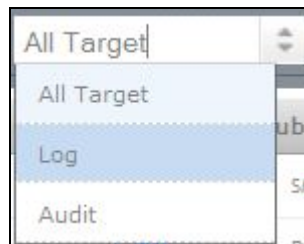


Figure 11. Target Filter

It allows filtering Whole Log List by Target.

It shows searched result by selected target.

For example, if “Log” is selected, user can see only logs.

- Host Filter



Figure 12. Host Filter

Allow filtering Whole Log List by name or address of host.

It shows searched result by selected host.

For example, if you enter 192.168.1.103, logs and audits containing 192.168.1.103 as its source or target IP address are filtered.

Or you can specify host name “powercom” instead of its IP address.

- Page Filter

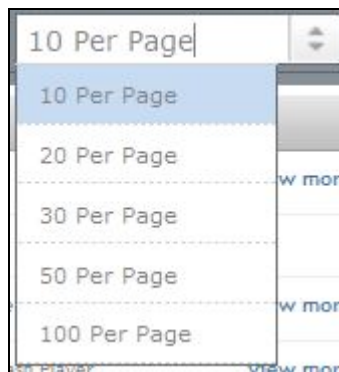


Figure 13. Page Filter

Filter Whole Log List by Page.

User can see only log as much as selected number.

For example, if selected 10 per Page, you can see 10 logs in one page.

4.1.2 ICMP

Show list of stored ICMP Communication Logs in selected DB.

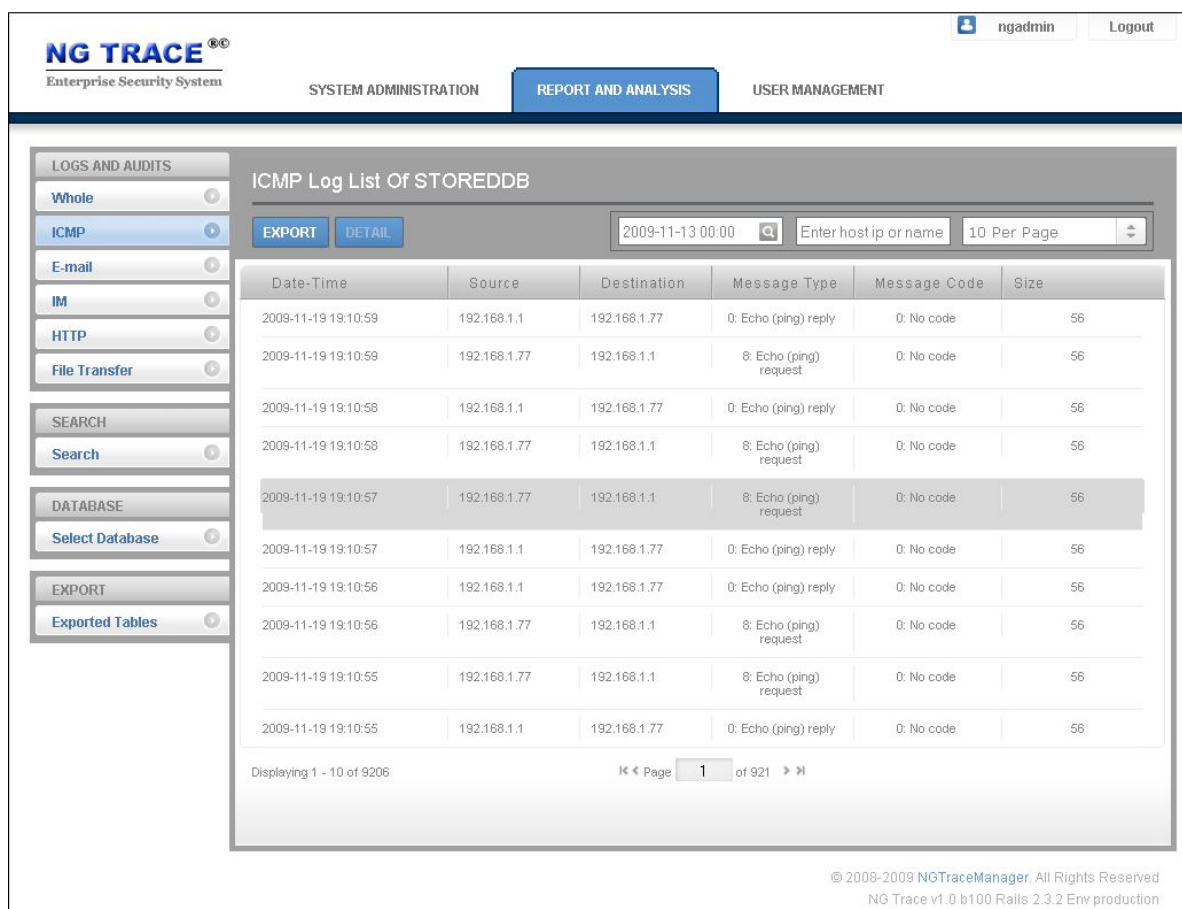


Figure 14. ICMP Log List

The following information indicates contents of recorded ICMP log.

- Date – Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Message Type: ICMP message type.
- Message Code: Message code information.
- Size: ICMP packet length.

Can filter ICMP Log List by Date-Time, Host, Page.

2009-11-13 00:00 Enter host ip or name 10 Per Page

Figure 15. Result Filter of ICMP Log

- [EXPORT]
Export the ICMP Log as CSV file.

When receiving the following message, click OK, then ICMP Log is exported as CSV file.

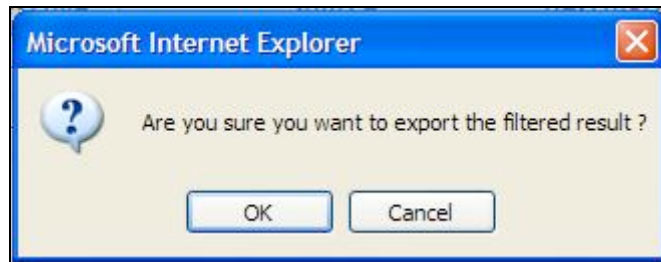


Figure 16. Export message.

- [DETAIL]
View detailed information of ICMP Log.

A screenshot of the NG TRACE Enterprise Security System web interface. The top navigation bar includes 'SYSTEM ADMINISTRATION', 'REPORT AND ANALYSIS' (which is highlighted), and 'USER MANAGEMENT'. On the right, there are links for 'ngadmin' and 'Logout'. The left sidebar contains several menu items: 'LOGS AND AUDITS' (with sub-items 'Whole', 'ICMP', 'E-mail', 'IM', 'HTTP', 'File Transfer'), 'SEARCH' (with 'Search'), 'DATABASE' (with 'Select Database'), and 'EXPORT' (with 'Exported Tables'). The main content area is titled 'ICMP Detail' and features a 'BACK' button. Below this is a table with two columns: 'Classific' and 'Contents'. The table contains the following data:

Classific	Contents
Date-Time:	2009-11-19 19:10:59
Source Address:	192.168.1.1
Destination Address:	192.168.1.77
Message Type:	0: Echo (ping) reply
Message Code:	0: No code
Size:	56
Information:	Echo (ping) reply: No code

Figure 17. ICMP Detail

4.1.3 E-mail

Display list of stored E-mail Communication Logs in selected DB.

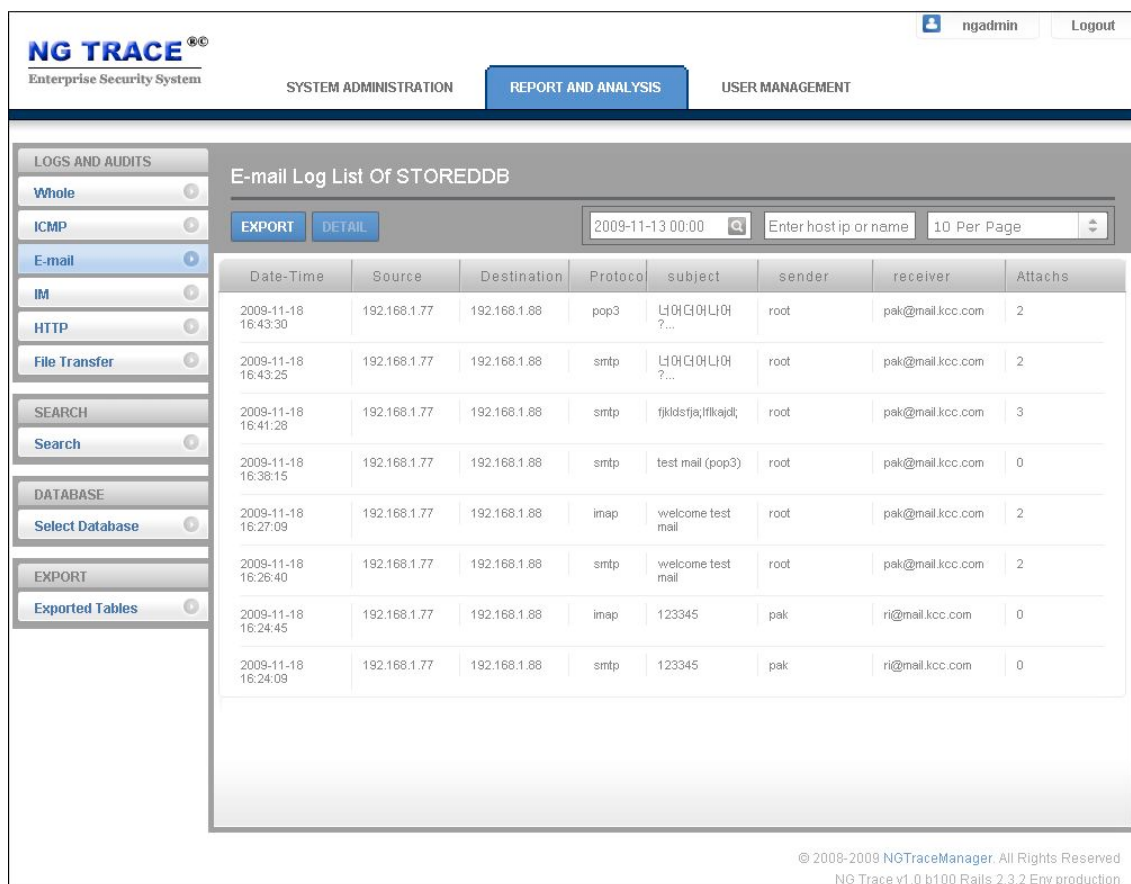


Figure 18. E-mail Log List

The following information indicates contents of recorded E-mail log.

- Date – Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Protocol: Type of E-mail.
- Subject: E-mail's subject.
- Sender: E-mail Sender.
- Receiver: E-mail Receiver.
- Attaches: Attached files.

Filter E-mail Log List by Date-Time, Host, and Page.

2009-11-13 00:00 Enter host ip or name 10 Per Page

Figure 19. Result Filter of E-mail Log

- [EXPORT]
Export the E-mail Log as CSV file.
When receiving the following message, click OK, then ICMP Log is exported as CSV file.

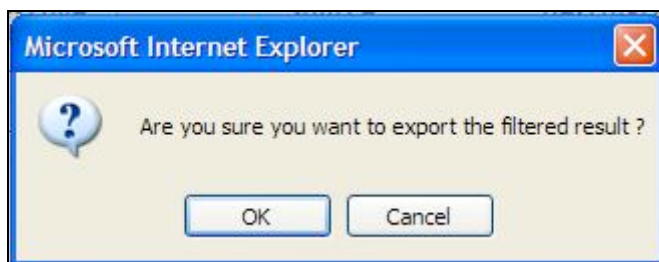


Figure 20. Export message.

- [DETAIL]
View detailed information of E-mail Log.

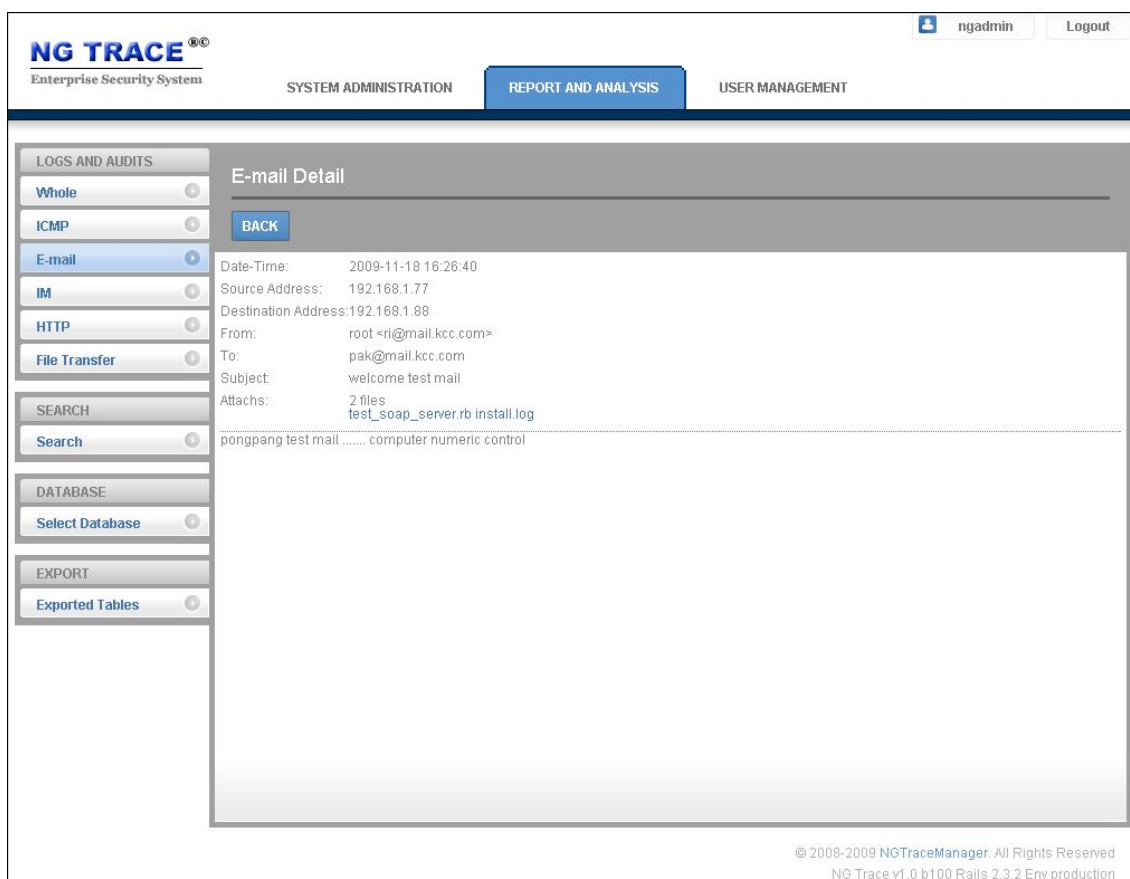


Figure 21. E-mail Detail.

4.1.4 IM

Display list of stored IM Communication Logs in selected DB.

NG TRACE[®]
Enterprise Security System

SYSTEM ADMINISTRATION REPORT AND ANALYSIS USER MANAGEMENT

LOGS AND AUDITS

- Whole
- ICMP
- E-mail
- IM**
- HTTP
- Ftp

SEARCH

Search

DATABASE

Select Database

EXPORT

Exported Tables

IM Log List Of STOREDDB

EXPORT 2008-09-03 00:00 All Hosts 10 Per Page

Date-Time	Source	Destination	Type	Server	Up/Down	Contents
2009-06-09 00:00:00	192.168.1.103	192.168.1.106	Skype	skype	Down	?? ??? ???
2009-08-12 11:15:03	192.168.1.107	192.168.1.101	JABBER	hahaha	Up	mt.exe

© 2008-2009 NGTraceManager. All Rights Reserved
NG Trace v1.0 b100 Rails 2.3.2 Env development

Figure 22. IM Log List

The following information indicates contents of recorded IM log.

- Date – Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Type: Sub type of IM protocol.
- Server: Name of Server.
- Up/Down: Upload/Download.
- Contents: Message text, file name.

Filter IM Log List by Date-Time, Host, and Page.



Figure 23. Result Filter of IM Log

- **[EXPORT]**
Export the IM Log as CSV file.
When receiving the following message, click OK, then ICMP Log is exported as CSV file.



Figure 24. Export message.

4.1.5 HTTP

Display list of stored HTTP Communication Logs in selected DB.

NG TRACE Enterprise Security System

ngadmin Logout

SYSTEM ADMINISTRATION **REPORT AND ANALYSIS** USER MANAGEMENT

LOGS AND AUDITS

- Whole
- ICMP
- E-mail
- IM
- HTTP**
- File Transfer

SEARCH

Search

DATABASE

Select Database

EXPORT

Exported Tables

HTTP Log List Of RECENTDB- 192.168.1.144

EXPORT DETAIL 2009-11-13 00:00 Enter hostip or name 10 Per Page

Date-Time	Source	Destination	Method	URL
2009-11-20 15:06:47	192.168.1.88	192.168.1.144	GET	http://192.168.1.144/fs/file/index.php?img=favicon
2009-11-20 15:06:37	192.168.1.88	192.168.1.144	GET	http://192.168.1.144/fs/file/view?path=%27ngt_telxKk_filePh...
2009-11-20 15:06:22	192.168.1.88	192.168.1.202	GET	http://192.168.1.202/report/Report/contents?proto=4&id=9745
2009-11-20 15:04:40	192.168.1.88	192.168.1.34	GET	http://192.168.1.34/mysois
2009-11-20 15:03:51	192.168.1.88	192.168.1.202	GET	http://192.168.1.202/report/report/?proto=4
2009-11-20 15:03:39	192.168.1.88	192.168.1.34	GET	http://192.168.1.34/mysois/
2009-11-20 15:03:38	192.168.1.88	192.168.1.34	GET	http://192.168.1.34/index.html
2009-11-20 15:03:11	192.168.1.88	192.168.1.202	GET	http://192.168.1.202/networkadmin/exe_components

© 2008-2009 NGTraceManager. All Rights Reserved.
NG Trace v1.0 b100 Rails 2.3.2 Env production

Figure 25. HTTP Log List

The following information indicates contents of recorded IM log.

- Date – Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Method: HTTP method.
- URL: URL of visit web site.
- Cookie: Cookie information.

Filter HTTP Log List by Date-Time, Host, and Page.

2009-11-13 00:00 Enter hostip or name 10 Per Page

Figure 26. Result Filter of HTTP Log

- [EXPORT]
Export the HTTP Log as CSV file.

When receiving the following message, click OK, then ICMP Log is exported as CSV file.

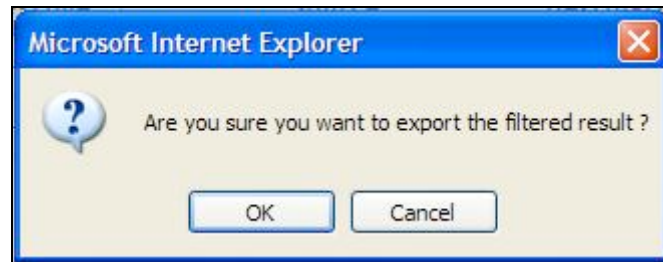


Figure 27. Export message.

- [DETAIL]
View detailed information of HTTP Log.

Classific	Contents
Date-Time:	2009-11-20 15:03:11
Source Address:	192.168.1.88
Destination Address:	192.168.1.202
Method:	GET
Cookie:	__source_session=BAh7DDoPc2Vzc2lvd9pZCllOTRlOTI3ZGFjY2MxY2NlZnZlRiYTMzMjZnZAwNDE6FG1vbml0b3Jfb3B0aWV9uc3sHOg1wZXJfcGFnZTA6CXBhZ2UwOWhoaWdoX2ZpbHRic9vcHRpb25zeA7BzA6DW9tdGFyZ2V0MD0Mb19jcm10aTA6D21vbml0b3JfaWQwOgxyX3Byb3RvMDsMD0Lb19uYVY1
Content Type:	text/html; charset=utf-8
URL:	http://192.168.1.202/networkadmin/exe_components
Information:	HTTP/1.0 [1.1 200:OK Response]

© 2008-2009 NGTraceManager. All Rights Reserved
NG Trace v1.0 b100 Rails 2.3.2 Env production

Figure 28. HTTP Detail

4.1.6 FTP

Display list of stored FTP Communication Logs in selected DB.

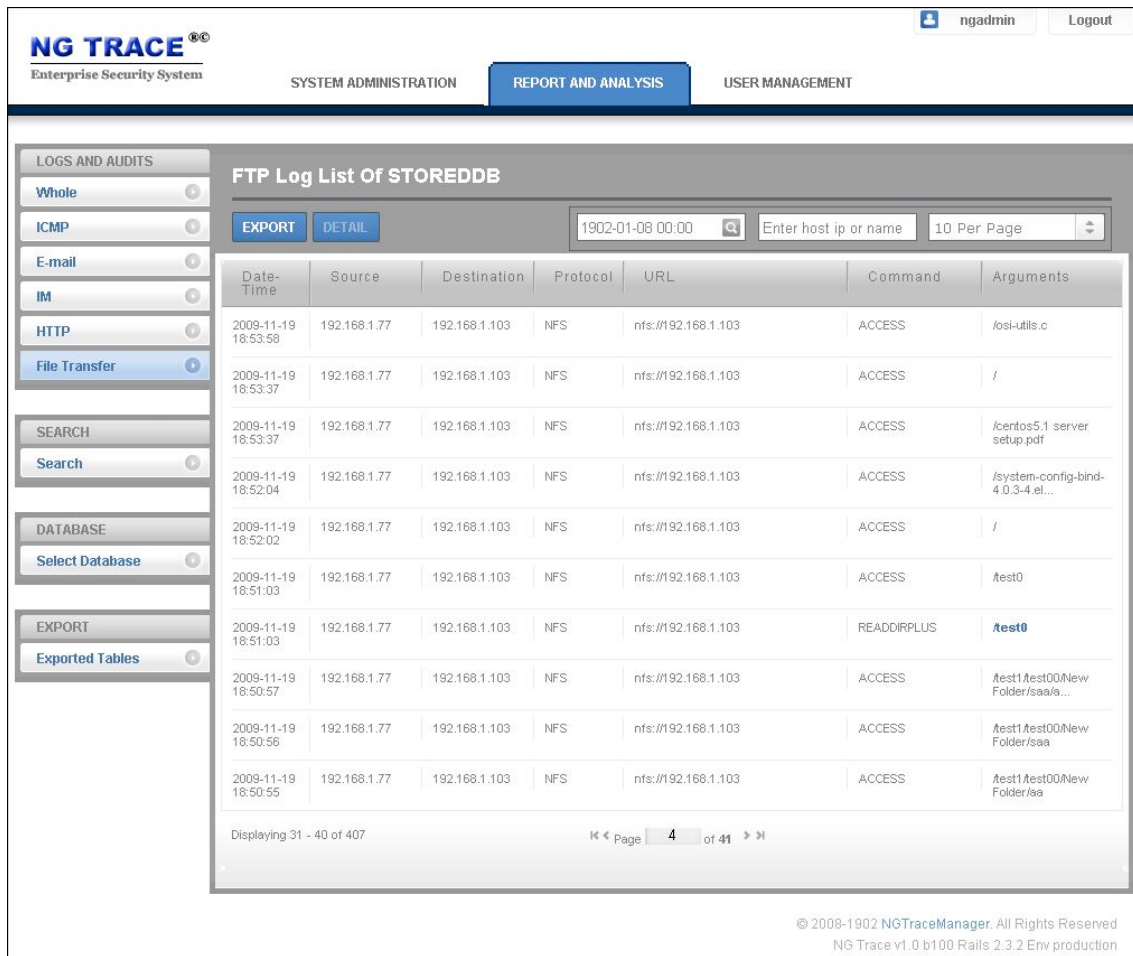


Figure 29. FTP Log List

The following information indicates contents of recorded FTP log.

- Date – Time: Captured time.
- Source: IP Address of Source.
- Destination: IP Address of Destination.
- Protocol: Type of file transfer protocol such as FTP and SMB
- URL: URL of visited web site
- Command: Request command.
- Arguments: Information of communication file.

Filter FTP Log List by Date-Time, Host, and Page.

2009-11-13 00:00

Enter host ip or name

10 Per Page

Figure 30. Result Filter of FTP Log

- [EXPORT]
Export the FTP Log as CSV file.
When receiving the following message, click OK, then ICMP Log is exported as CSV file.



Figure 31. Export message.

- [DETAIL]
View detailed information of FTP Log.

NG TRACE
Enterprise Security System

ngadmin Logout

SYSTEM ADMINISTRATION
REPORT AND ANALYSIS
USER MANAGEMENT

LOGS AND AUDITS

- Whole
- ICMP
- E-mail
- IM
- HTTP
- File Transfer

SEARCH

- Search

DATABASE

- Select Database

EXPORT

- Exported Tables

FTP Detail

BACK

Classific	Contents
Protocol:	SMB
Date-Time:	2009-11-20 15:44:54
Source Address:	192.168.1.88
Destination Address:	192.168.1.33
URL:	smb://192.168.1.33/Test_Plan/test_file.txt
Command:	File Read/Copy
Arguments:	/test_file.txt
Information:	File Read, FID : 4000

© 2008-1902 NGTraceManager. All Rights Reserved
NG Trace v1.0 b100 Rails 2.3.2 Env production

Figure 32. FTP Detail

Console log could be shown slowly about large file.

4.2 Search

Search the audit data stored in stored Database by keyword and protocol.

The screenshot displays the NG TRACE Enterprise Security System interface. The top navigation bar includes 'SYSTEM ADMINISTRATION', 'REPORT AND ANALYSIS' (selected), and 'USER MANAGEMENT'. The left sidebar contains sections for 'LOGS AND AUDITS' (with options like Whole, ICMP, E-mail, IM, HTTP, File Transfer), 'SEARCH' (with a 'Search' button), 'DATABASE' (with a 'Select Database' button), and 'EXPORT' (with an 'Exported Tables' button). The main content area is titled 'Search Audits' and features a search input field containing 'mail', a dropdown for 'All Types', and a '10 Per Page' selector. Below this is a table of search results with columns: ID, Time, Source, Destination, Protocol, Rule, and Info. The table contains four rows of audit data, each with a 'view more' link. The footer of the interface shows copyright information: '© 2008-1902 NGTraceManager. All Rights Reserved' and 'NG-Trace v1.0 b100 Rails 2.3.2 Env production'.

ID	Time	Source	Destination	Protocol	Rule	Info
9421	2009-11-18 16:24:09	192.168.1.77	192.168.1.88	E-mail	Audit	"pak " send a mail to "ri@mail.kcc.com" view more
9422	2009-11-18 16:24:45	192.168.1.77	192.168.1.88	E-mail	Audit	"pak " send a mail to "ri@mail.kcc.com" view more
9423	2009-11-18 16:26:40	192.168.1.77	192.168.1.88	E-mail	Audit	"root " send a mail to "pak@mail.kcc.com" view more
9424	2009-11-18 16:27:09	192.168.1.77	192.168.1.88	E-mail	Audit	" " send a mail to " " view more

Figure 33. Search

Input the keyword, or select the protocol and press .

4.3 Database

Display Database list that connect to System.

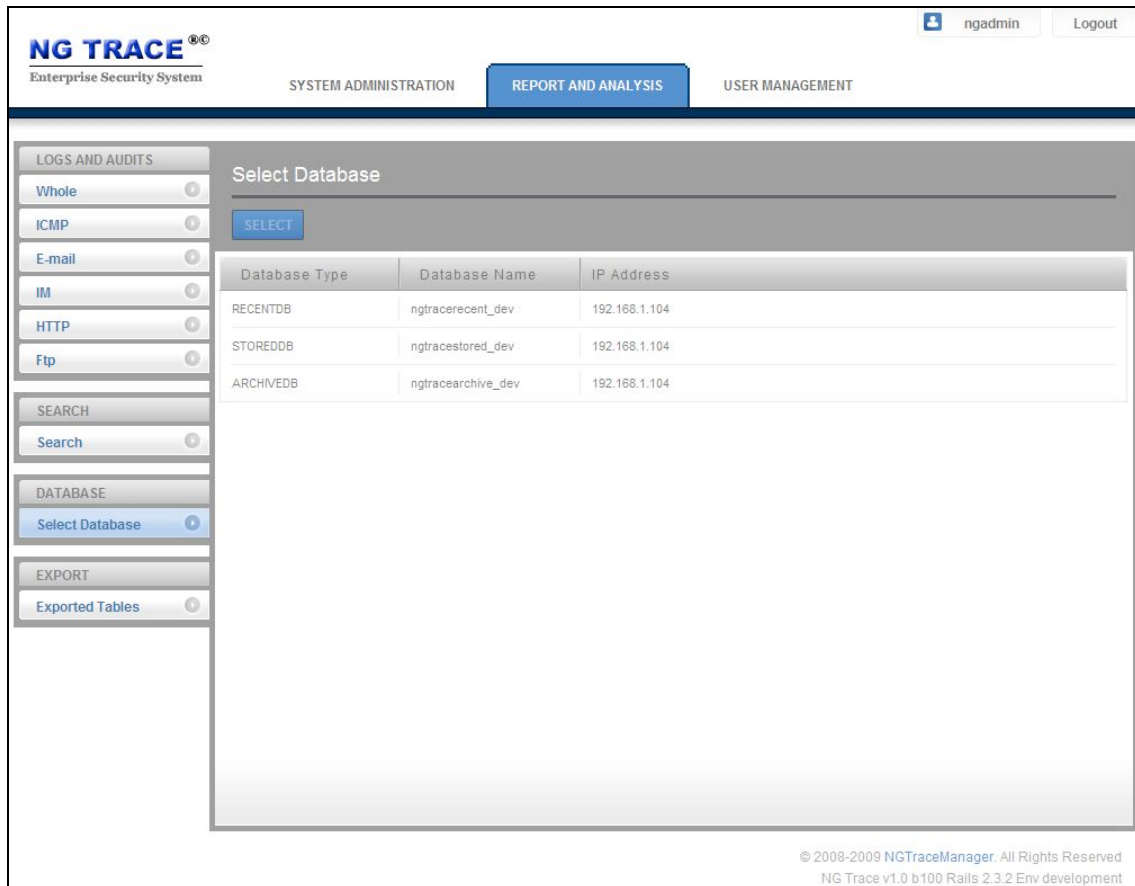


Figure 34. Select Database

- [SELECT]

From database list, select specific database to view stored log in it. If you select the RECENTDB and press the [SELECT], user can see Whole Log List stored in Recent DB.

Enterprise Security System

ngadmin

Logout

SYSTEM ADMINISTRATION

REPORT AND ANALYSIS

USER MANAGEMENT

LOGS AND AUDITS

Whole

ICMP

E-mail

IM

HTTP

Ftp

SEARCH

Search

DATABASE

Select Database

EXPORT

Exported Tables

Whole Log List Of RECENTDB- 192.168.1.104

2008-09-03 00:00

All Protocols

All Target

All Hosts

10 Per Page

Date-Time	Source	Destination	Protocol	Sub Type	Rule	Info
2009-03-15 00:00:00	192.168.1.105	192.168.1.1	E-mail	SMTP	Audit	???, ?? view more
2009-03-15 00:00:00	192.168.1.108	192.168.1.101	E-mail	POP3	Log	?? ?? ????
2009-04-21 00:00:00	192.168.1.106	192.168.1.101	FTP	FTP	Audit	stacraft.exe view more
2009-05-23 00:00:00	192.168.1.107	192.168.1.101	HTTP	HTTP	Audit	Download Flash Player view more
2009-06-09 00:00:00	192.168.1.103	192.168.1.106	IM	ICQ	Audit	??, ?? ??
2009-06-09 00:00:00	192.168.1.107	192.168.1.101	FTP	FTP	Log	?? ?? ????
2009-06-09 00:00:00	192.168.1.107	192.168.1.101	FTP	FTP	Log	?? ?? ????
2009-06-09 00:00:00	192.168.1.107	192.168.1.101	FTP	FTP	Log	?? ?? ????
2009-06-09 00:00:00	192.168.1.107	192.168.1.101	FTP	FTP	Log	?? ?? ????
2009-06-09 00:00:00	192.168.1.107	192.168.1.101	FTP	FTP	Log	?? ?? ????

Displaying 1 - 10 of 23

1

of 3

© 2008-2009 NGTraceManager. All Rights Reserved

NG Trace v1.0 b100 Rails 2.3.2 Env development

Figure 35. Whole Log List Of RECENTDB

4.4 EXPORT

Display exported file's list.

Enterprise Security System

ngadmin

Logout

SYSTEM ADMINISTRATION

REPORT AND ANALYSIS

USER MANAGEMENT

LOGS AND AUDITS

Whole

ICMP

E-mail

IM

HTTP

Ftp

SEARCH

Search

DATABASE

Select Database

EXPORT

Exported Tables

Exported Table List

DOWNLOAD

DELETE

DELETE ALL

File Name	Exported Date	Filter Condition
export-ftplogs-20090903213306-1.csv	2009-09-03 21:33:06	Protocol:FTP, From Time: 2008-09-03 00:00
export-ftplogs-20090903213328-1.csv	2009-09-03 21:33:28	Protocol:FTP, From Time: 2008-09-03 00:00
export-ftplogs-20090903213348-1.csv	2009-09-03 21:33:48	Protocol:FTP, From Time: 2008-09-03 00:00

© 2008-2009 NGTraceManager. All Rights Reserved

NG Trace v1.0 b100 Rails 2.3.2 Env development

Figure 36. Export Table List

The following information indicates contents of exported file.

- File Name: Name of exported file.
 - Exported Date: Exported date.
 - Filter Condition: Filter condition of exported file.
- [DOWNLOAD]
Download selected file.
 - [DELETE]
Delete selected file.
 - [DELETE ALL]
Delete all file.