NG Trace

User Manual

December 2009

Table of Contents

Table of Figures

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, t he 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 suspi cious or potentially dangerous events.

NG Trace as any modern security system is with flexible, multil ayered 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 us ers' 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 com patible 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.

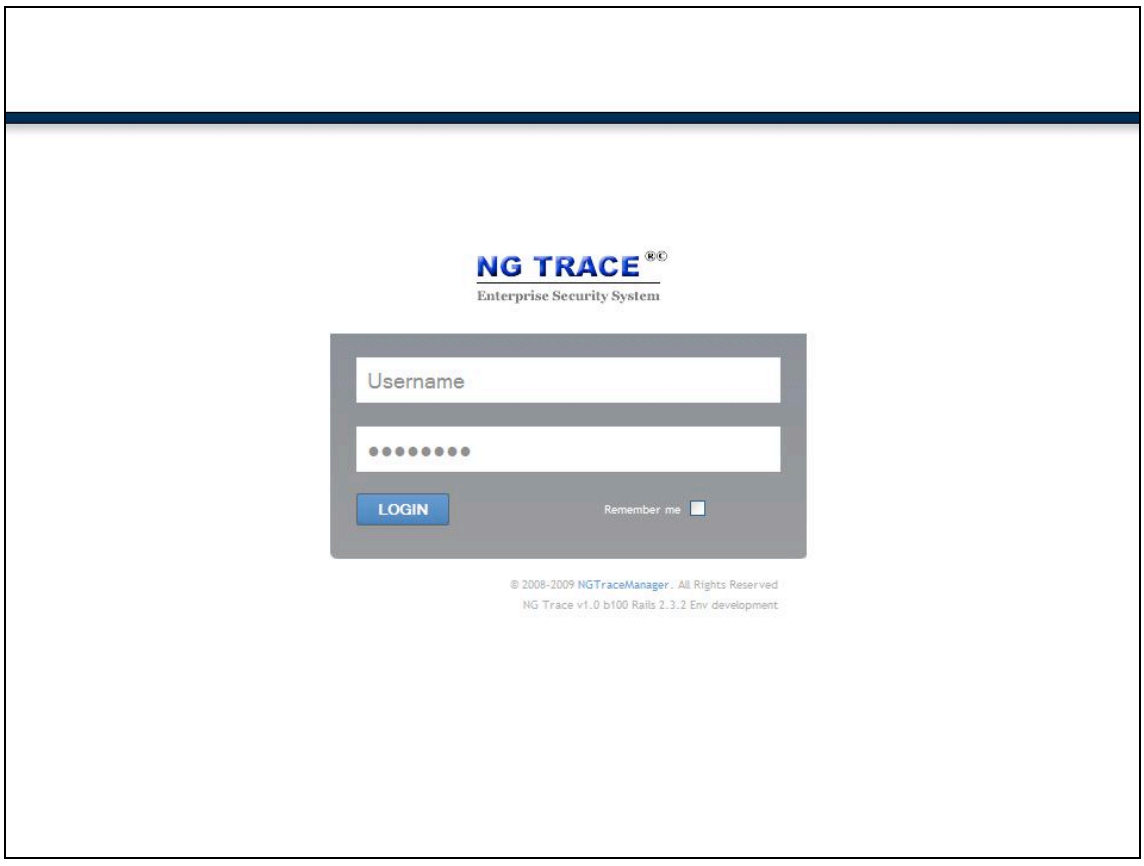

Figure 1. User Log In

3.2 User Management

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

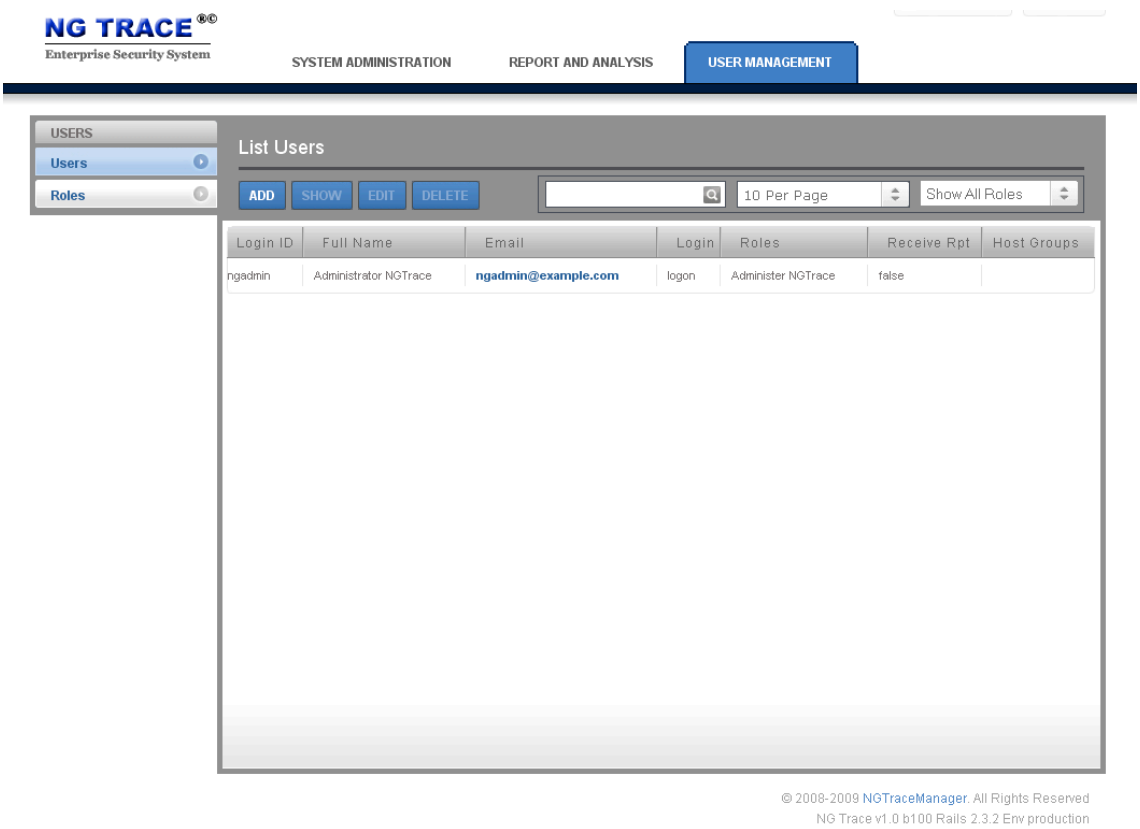

Figure 2. User Management Tab

User information contains user login ID, user name, e-mail address, phone nu mber, registered date, modified date, option whether or not to receive notify i nformation 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.

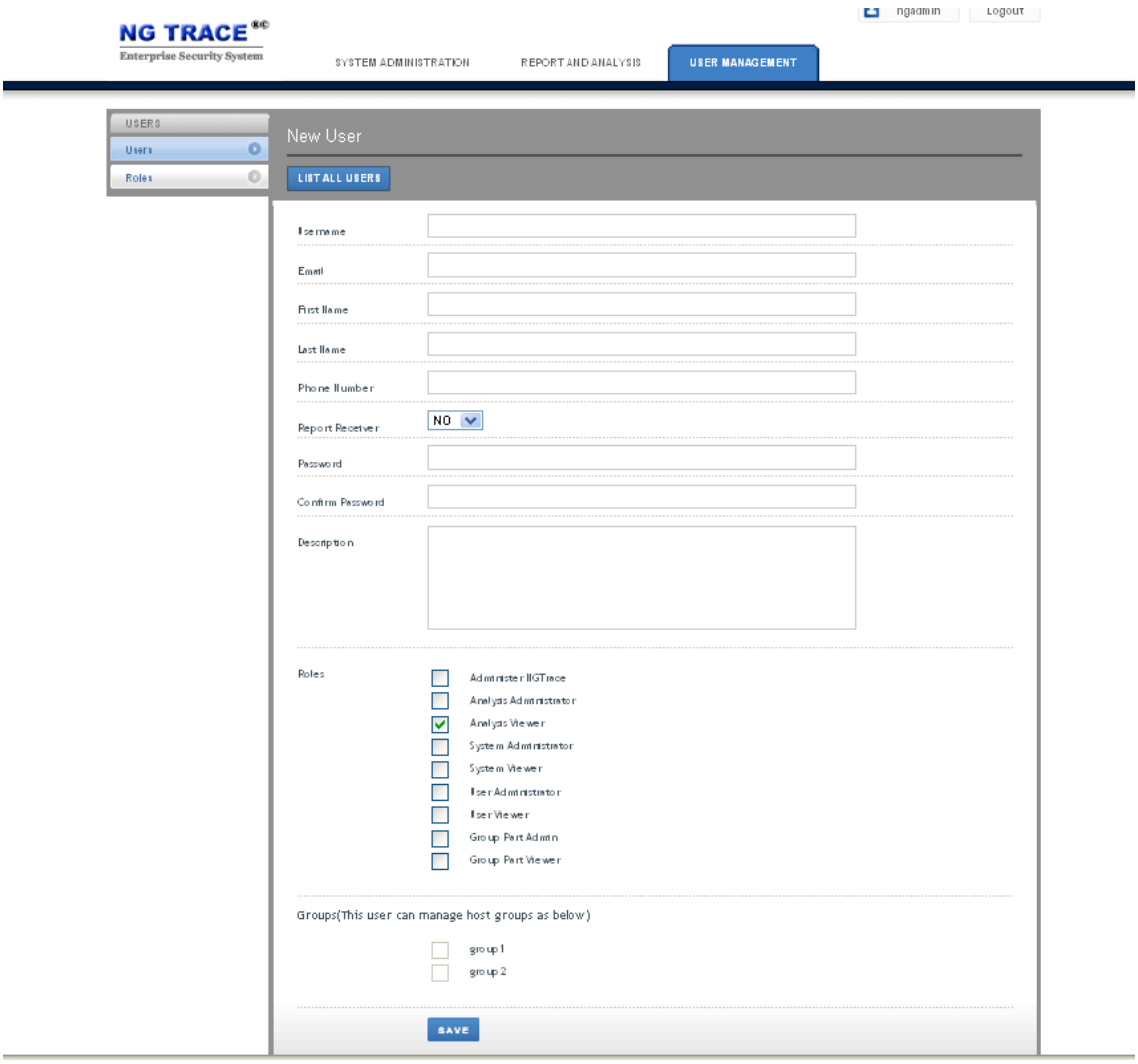

Figure 3. Add User

- [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.

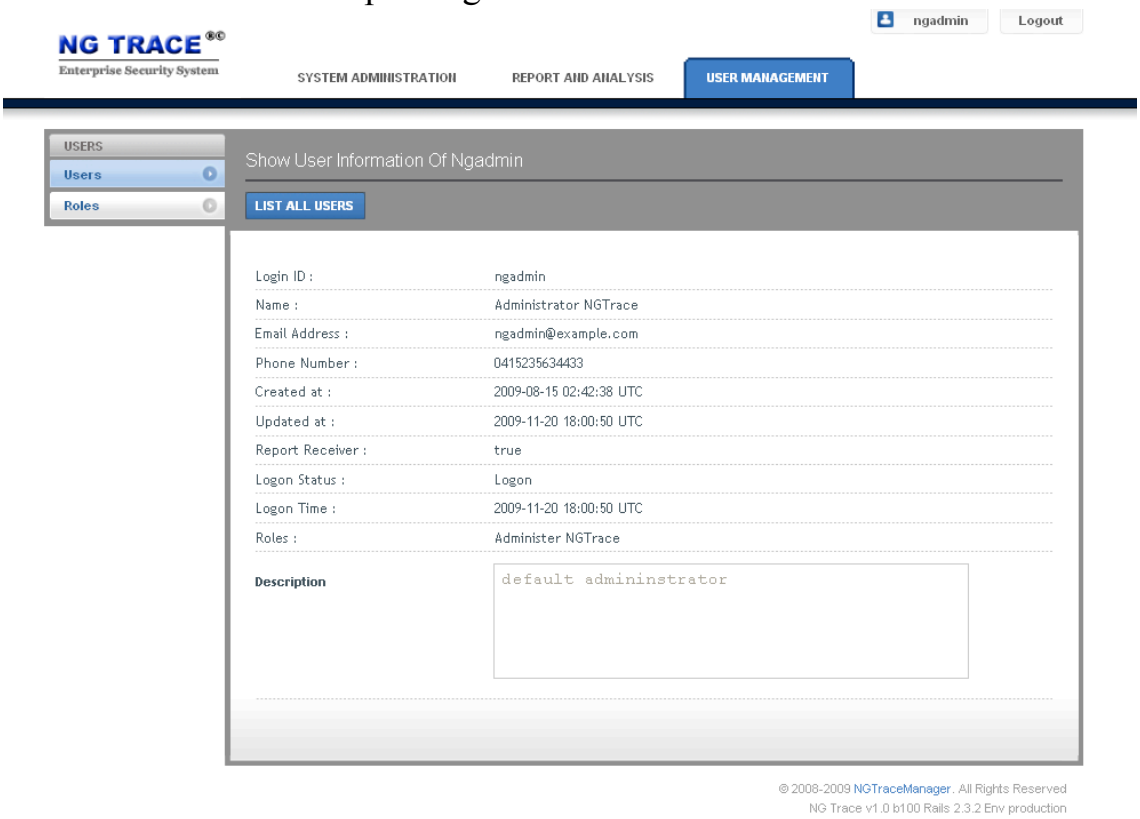

Figure 4. Show User Information

- [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.

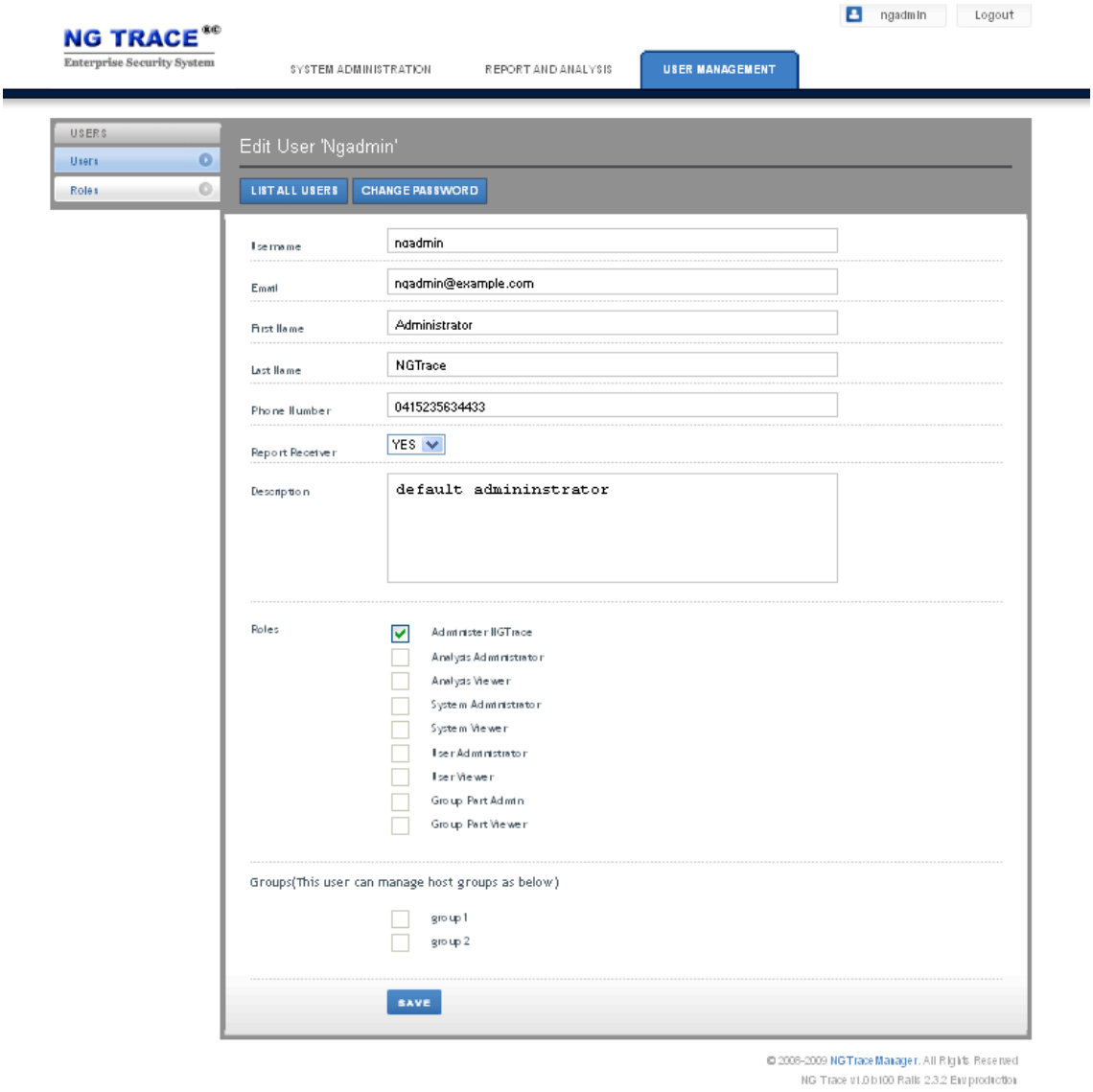

Figure 5. Edit User

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

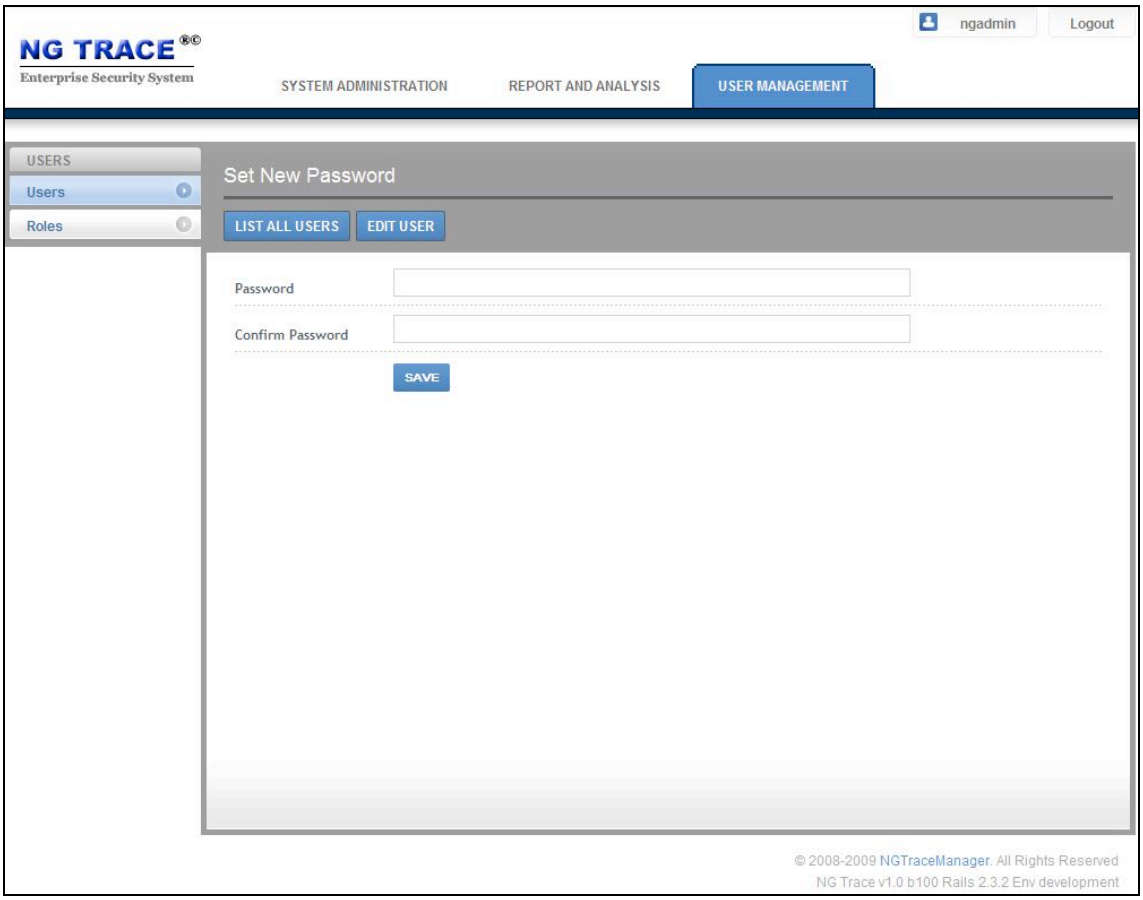

Figure 6. Set New Password

- [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.

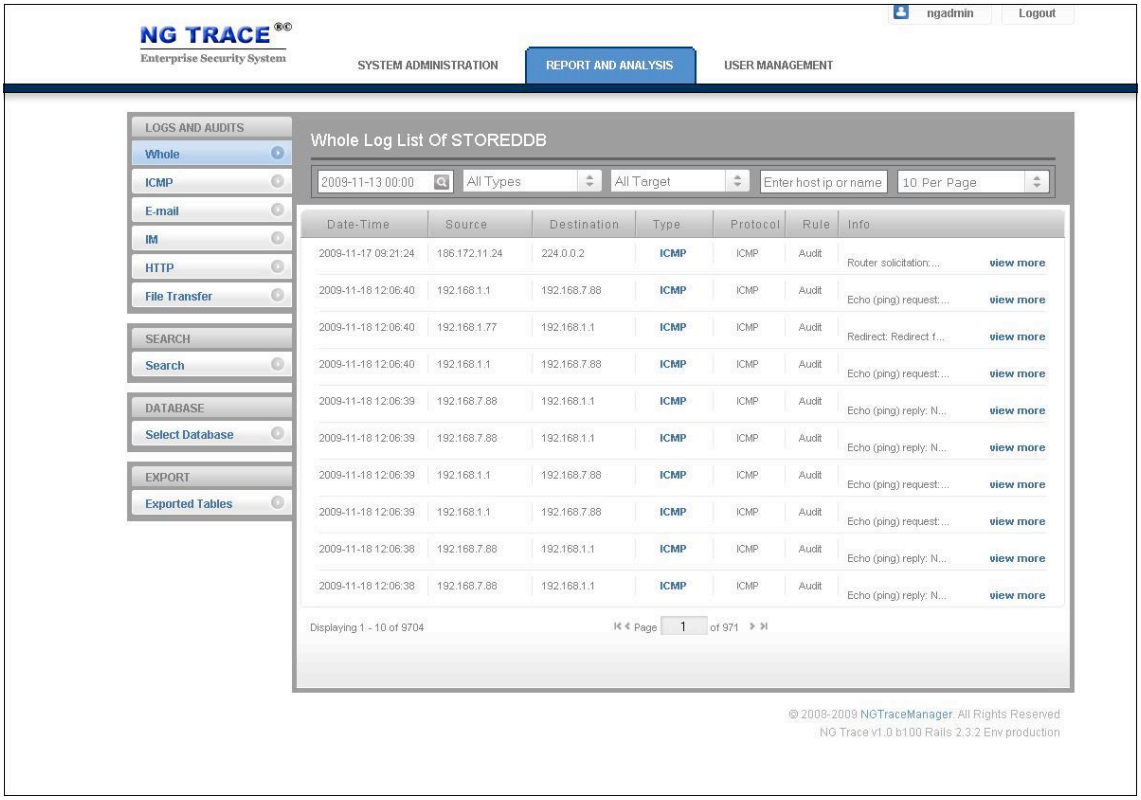

Figure 7. Whole Log List

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

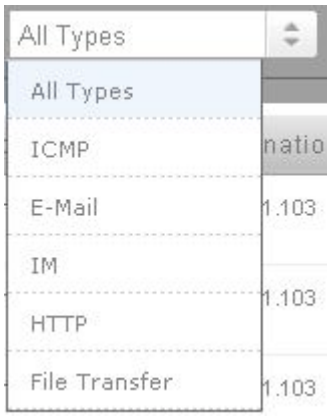

Figure 10. Protocol Filter

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

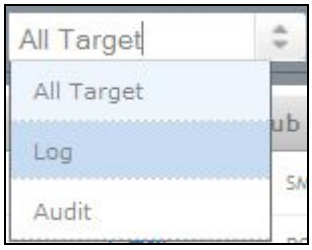

Figure 11. Target Filter

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

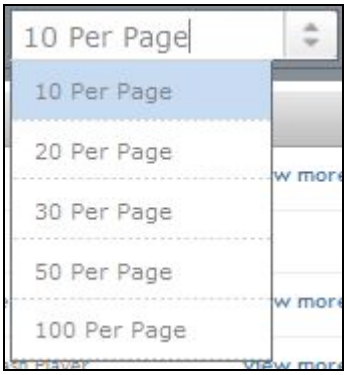

Figure 13. Page Filter

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.

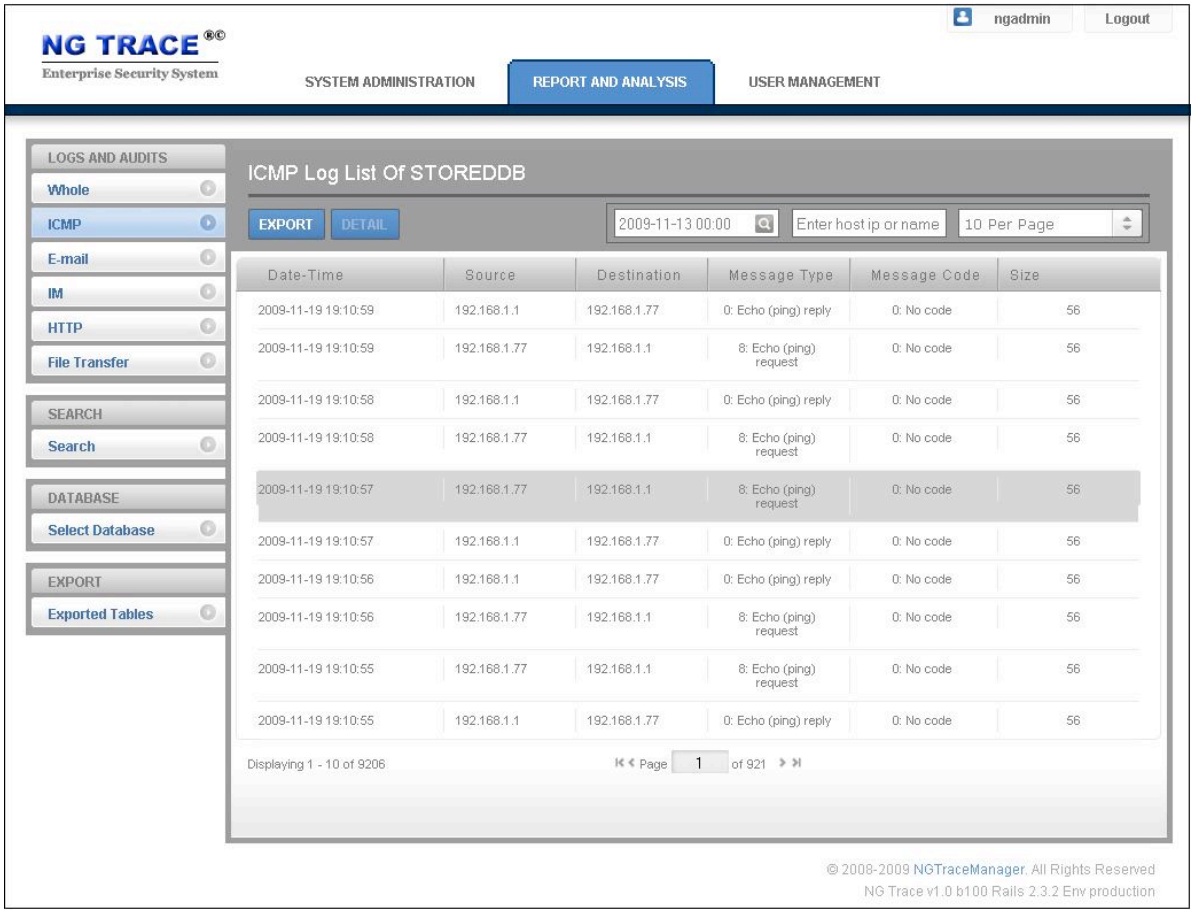

Figure 14. ICMP Log List

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.

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.

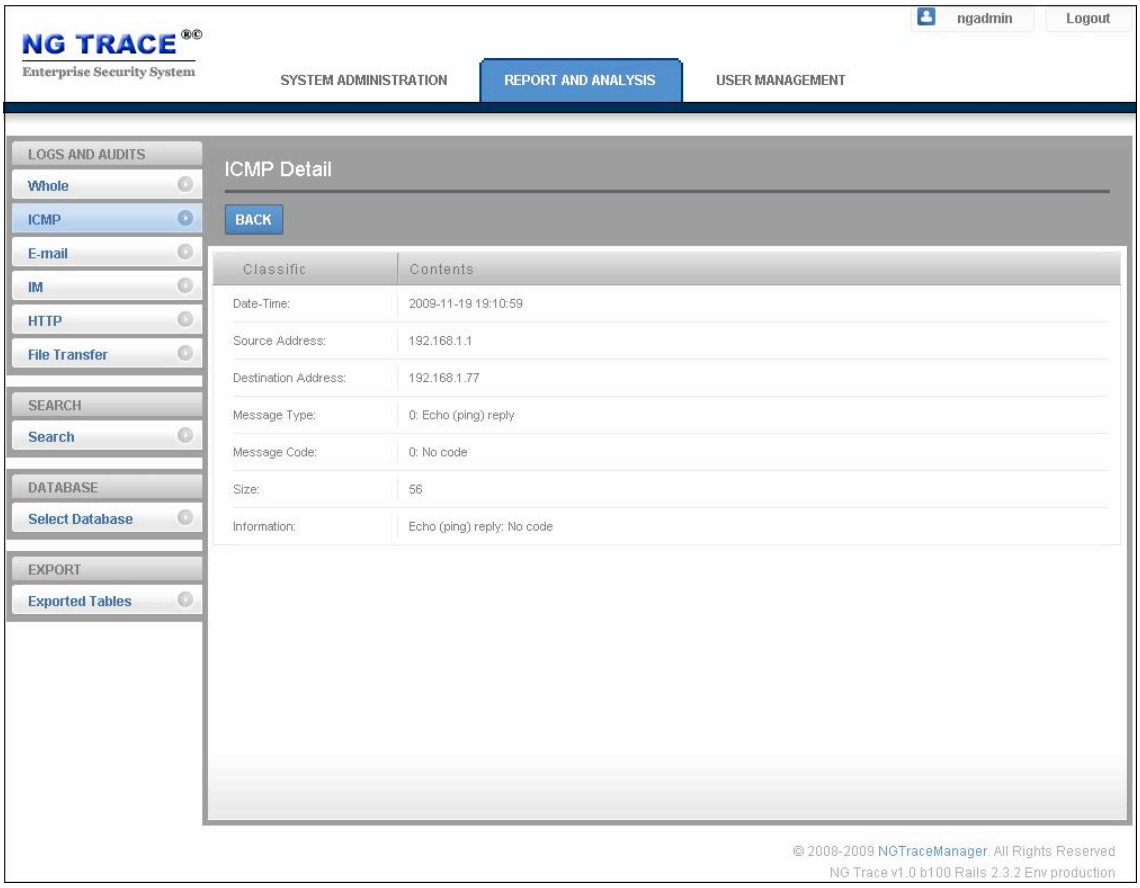

Figure 17. ICMP Detail

4.1.3 E-mail

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

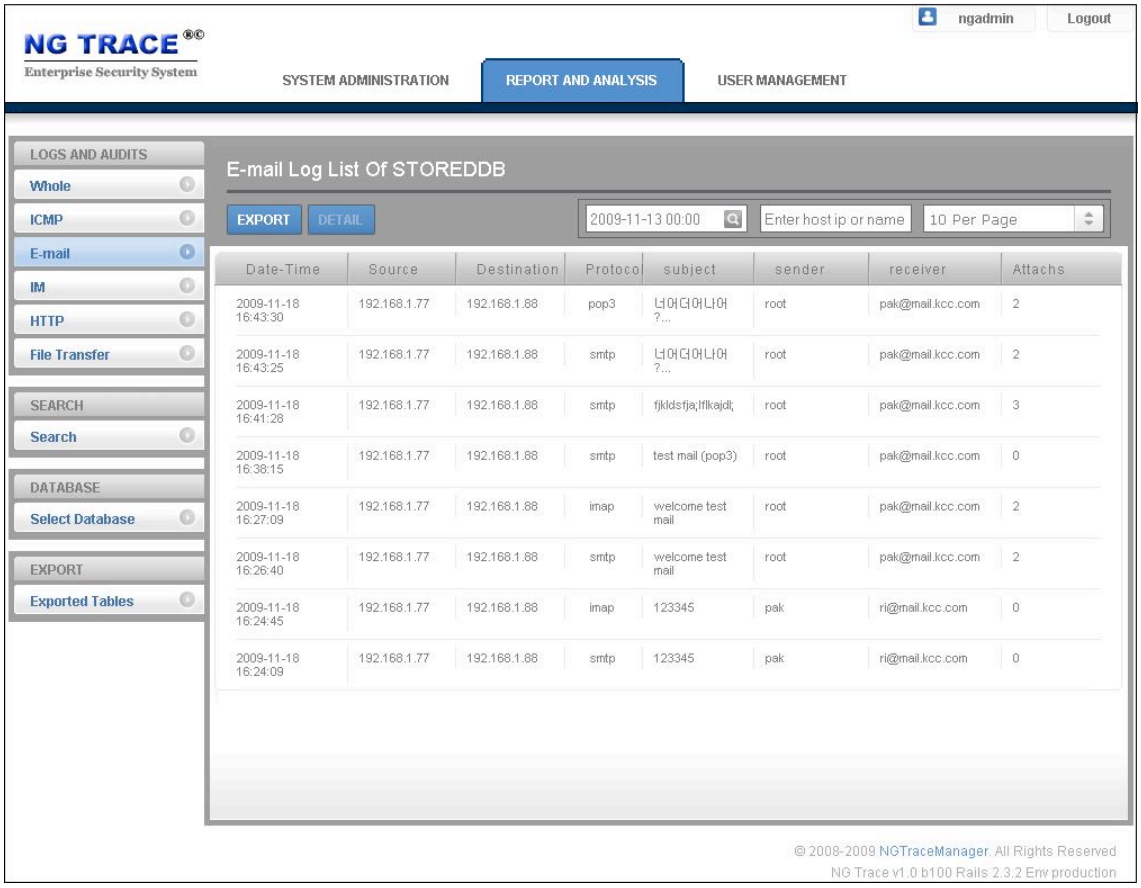

Figure 18. E-mail Log List

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.

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.

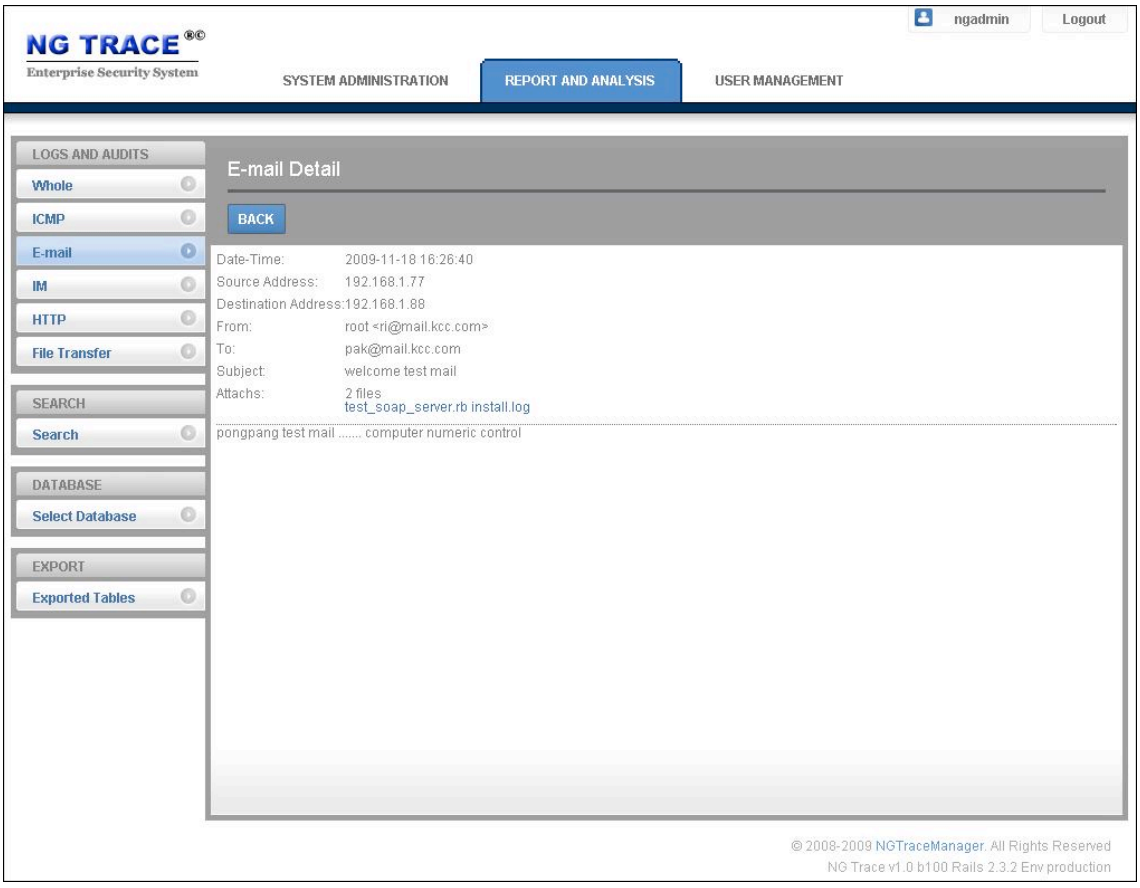

Figure 21. E-mail Detail.

4.1.4 IM

Display list of stored IM Communication Logs in selected DB.

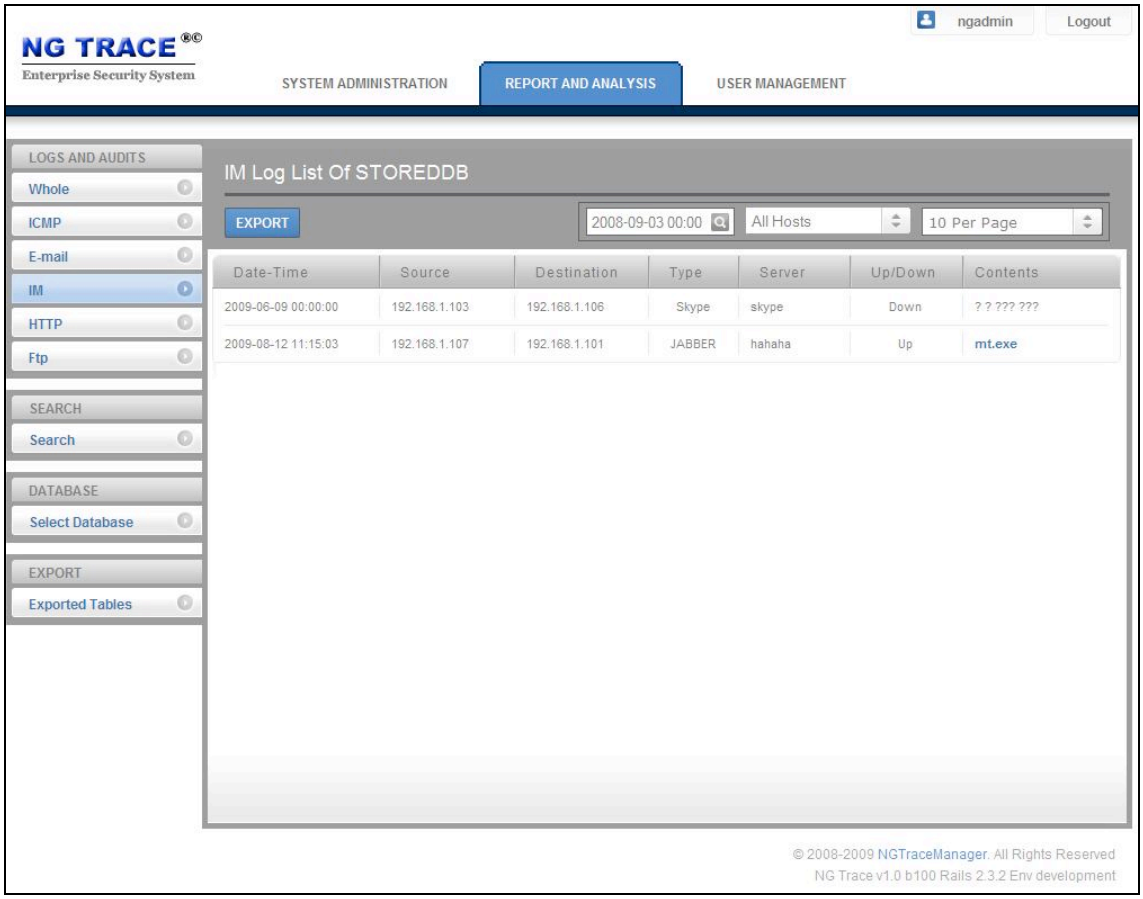

Figure 22. IM Log List

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.

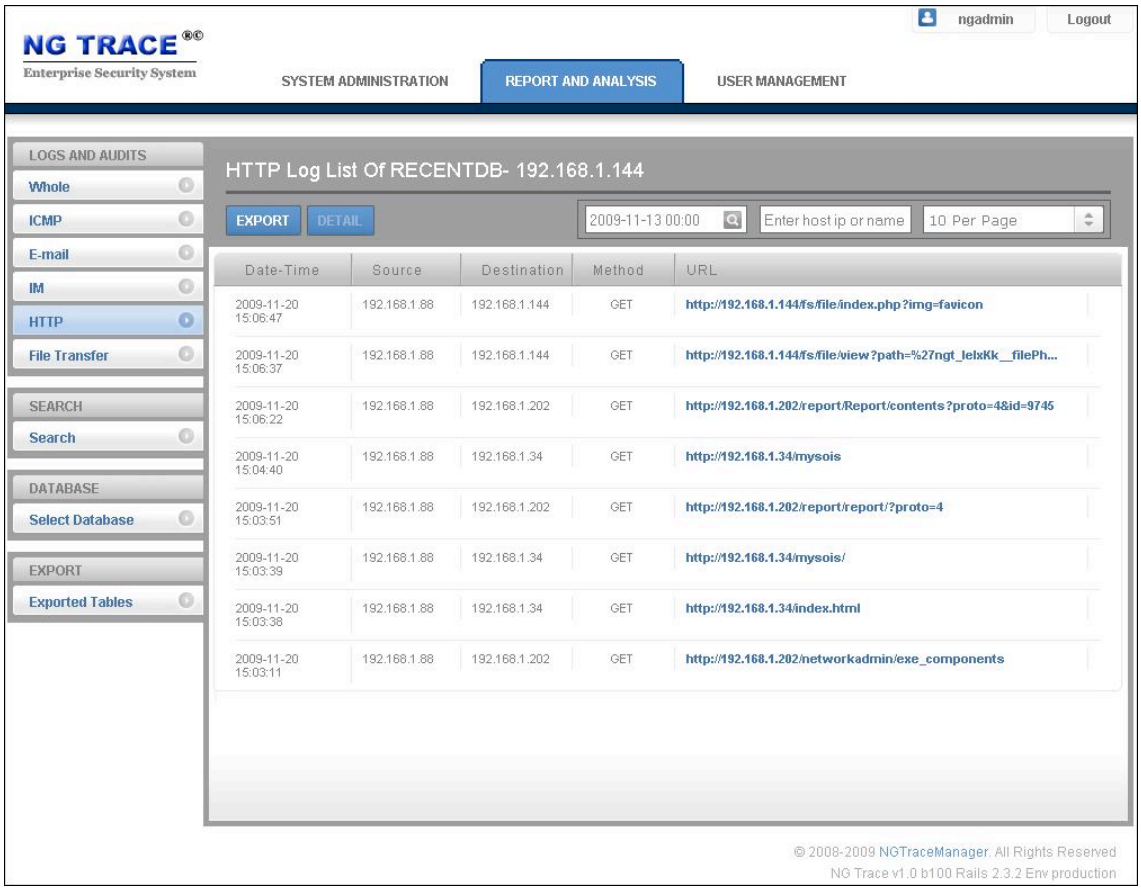

Figure 25. HTTP Log List

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.

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.

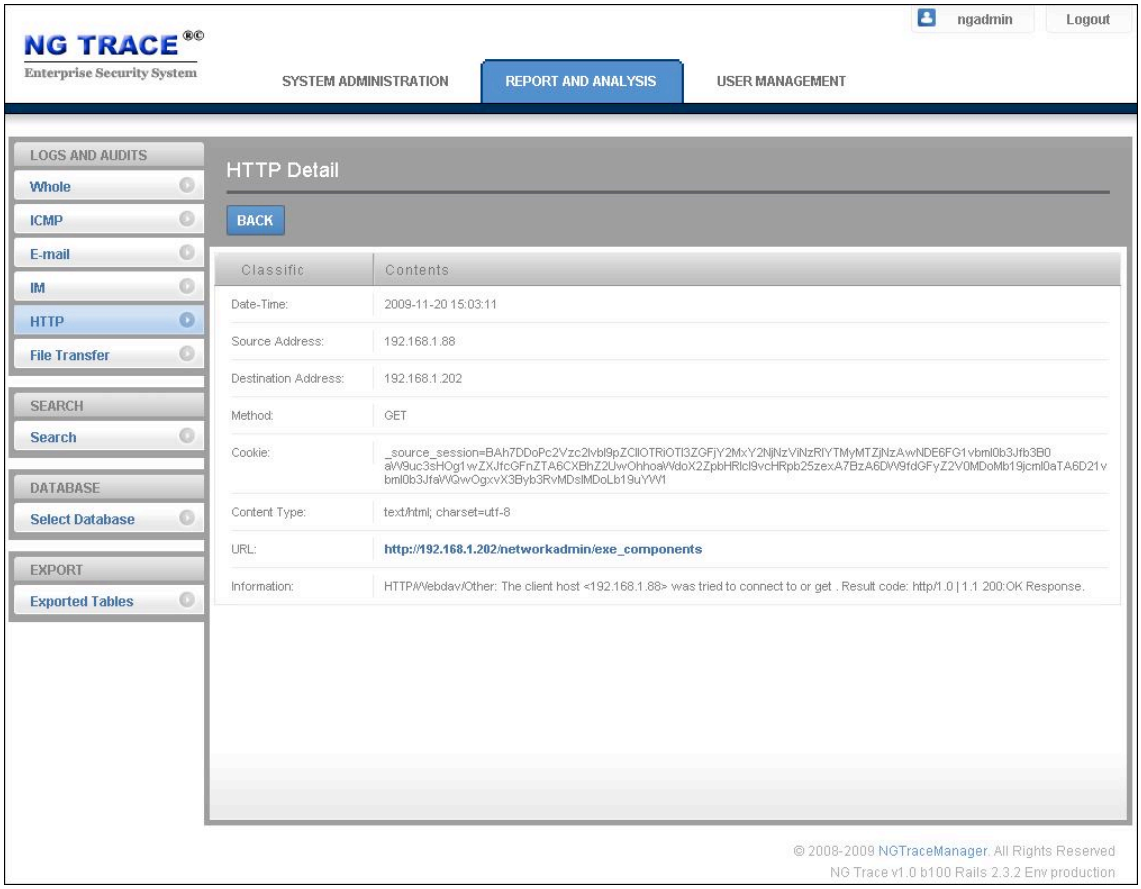

Figure 28. HTTP Detail

4.1.6 FTP

Display list of stored FTP Communication Logs in selected DB.

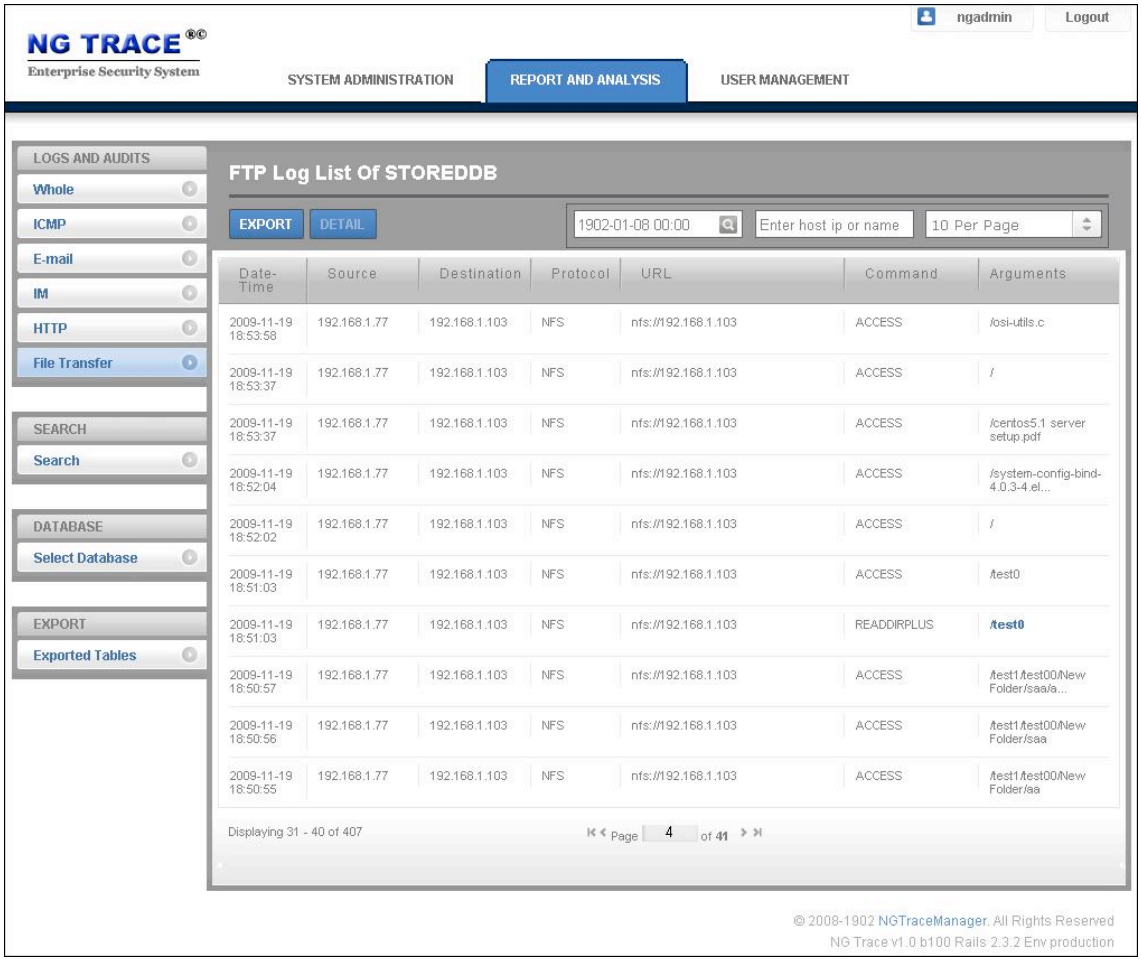

Figure 29. FTP Log List

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.

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.

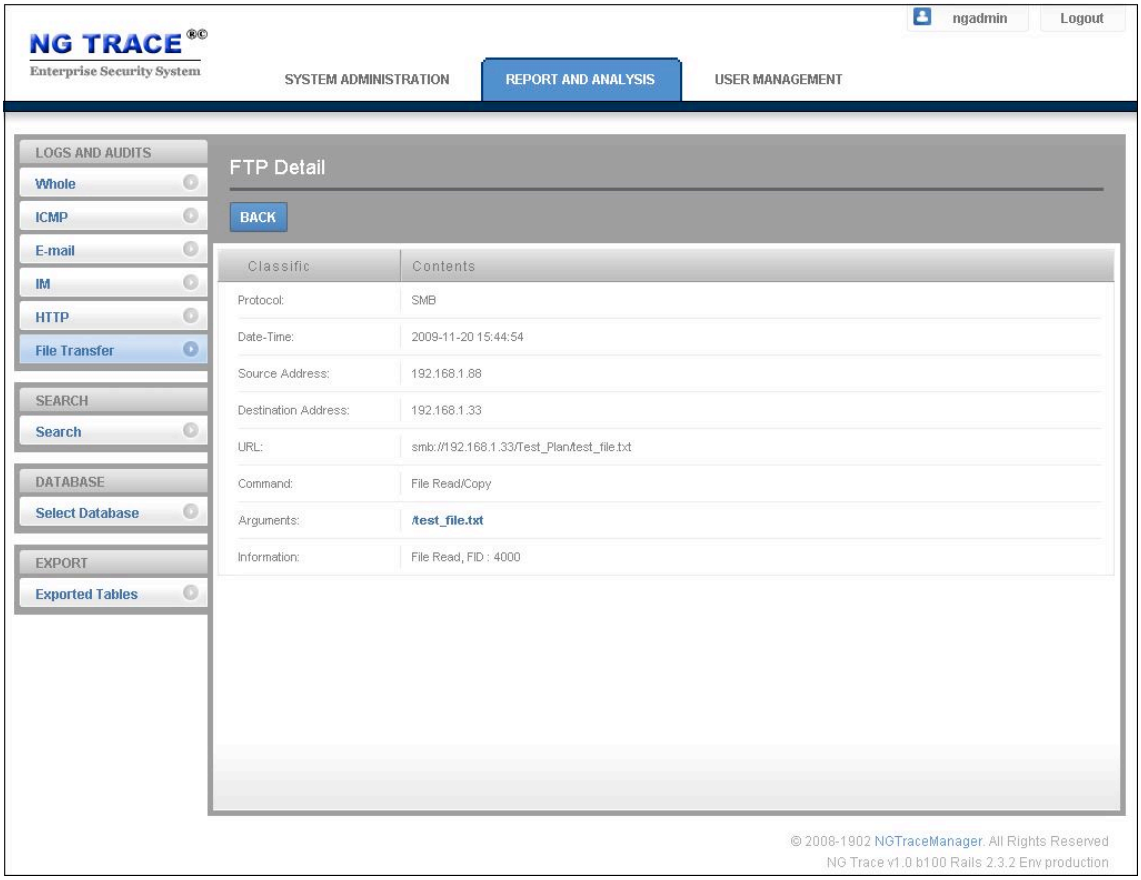

Figure 32. FTP Detail

Console log could be shown slowly about large file.

4.2 Search

Search the audit data stored in stored Database by keyword and prot ocol.

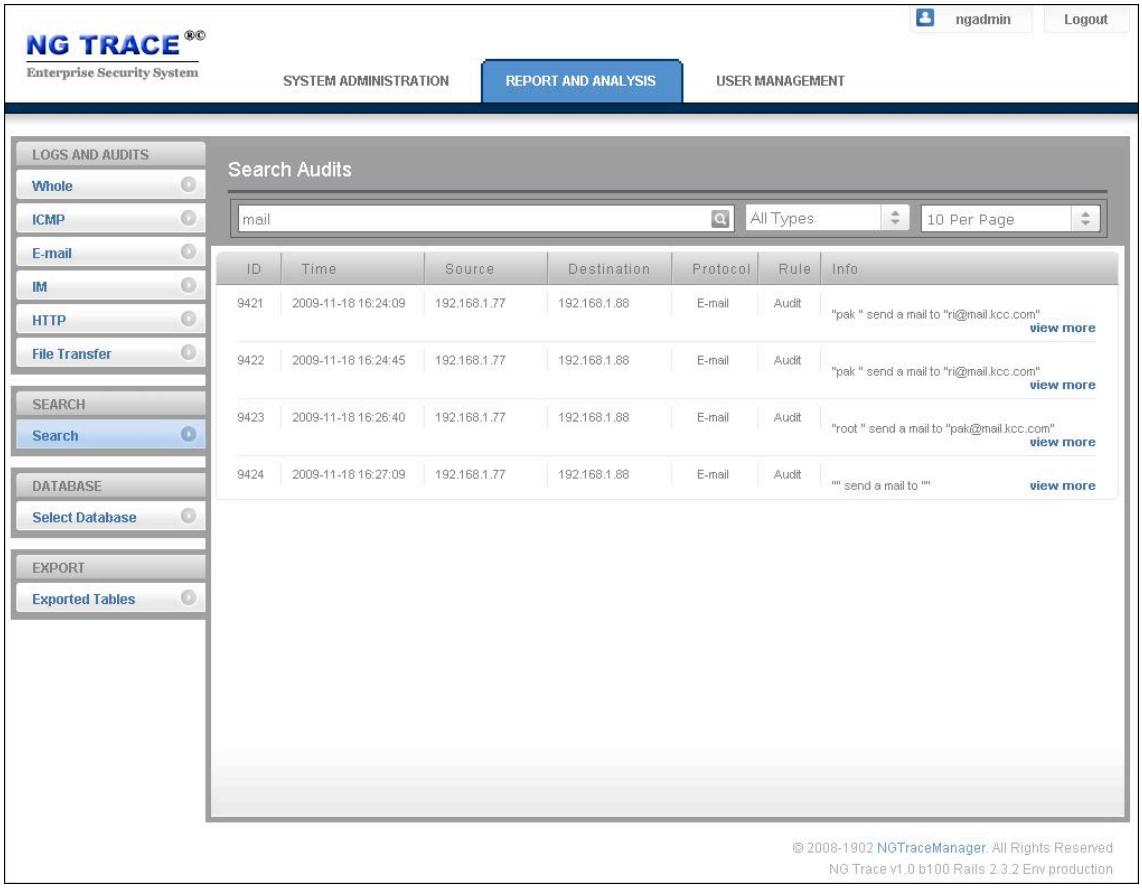

Figure 33. Search

Input the keyword, or select the protocol and press  .

4.3 Database

Display Database list that connect to System.

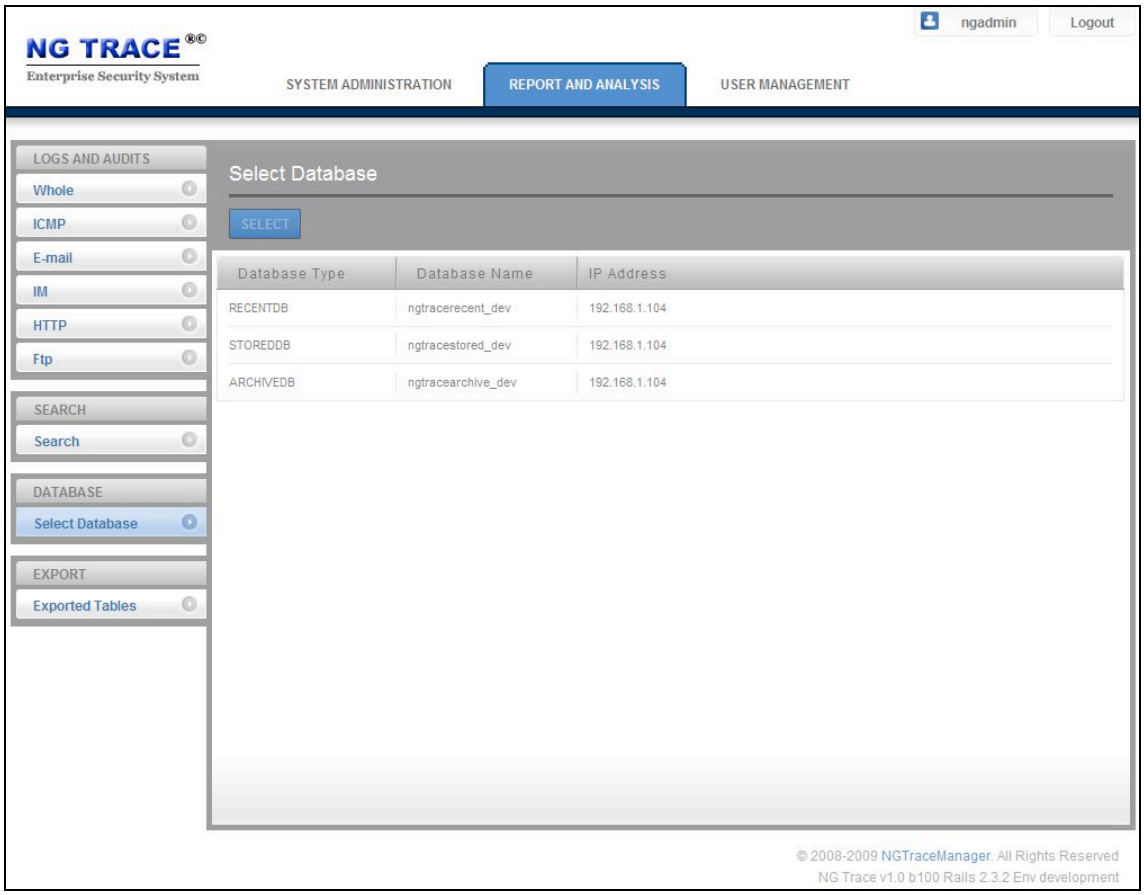

Figure 34. Select Database

- [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.

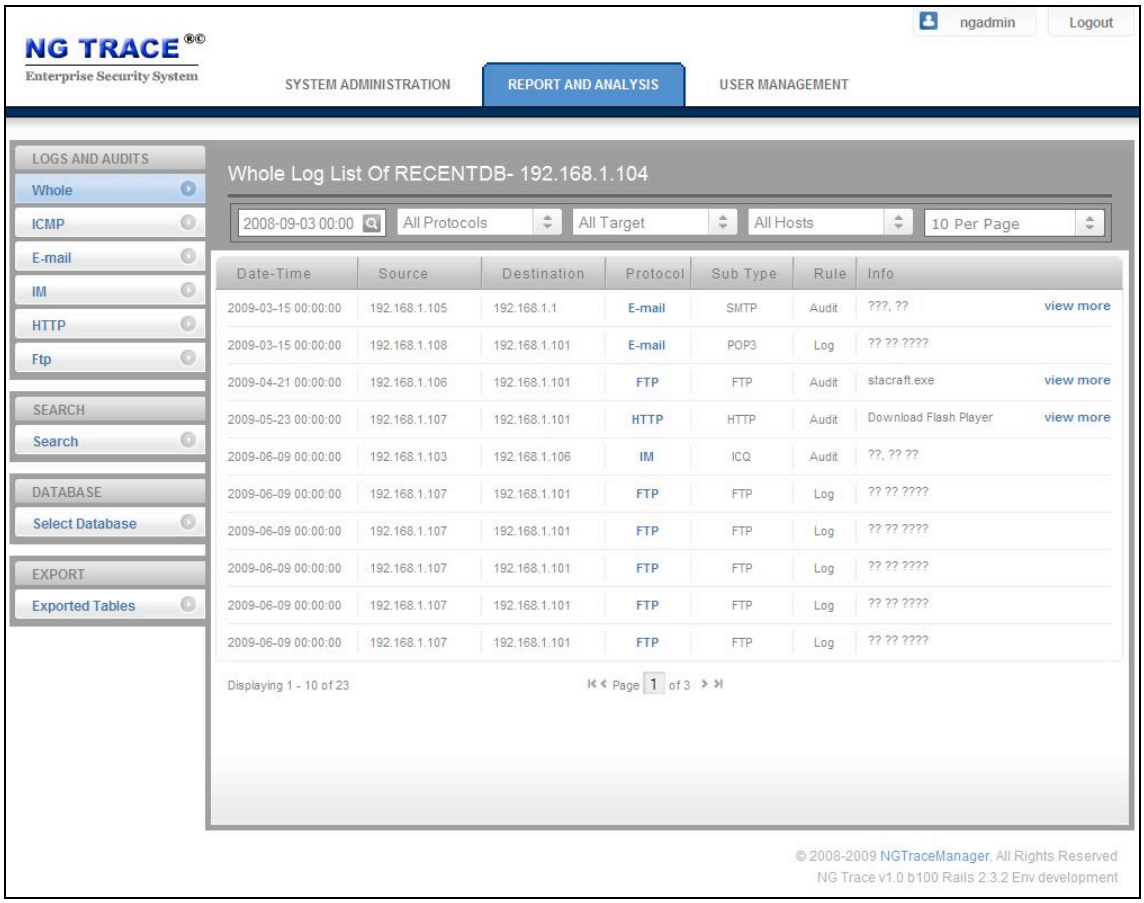

Figure 35. Whole Log List Of RECENTDB

4.4 EXPORT

Display exported file's list.

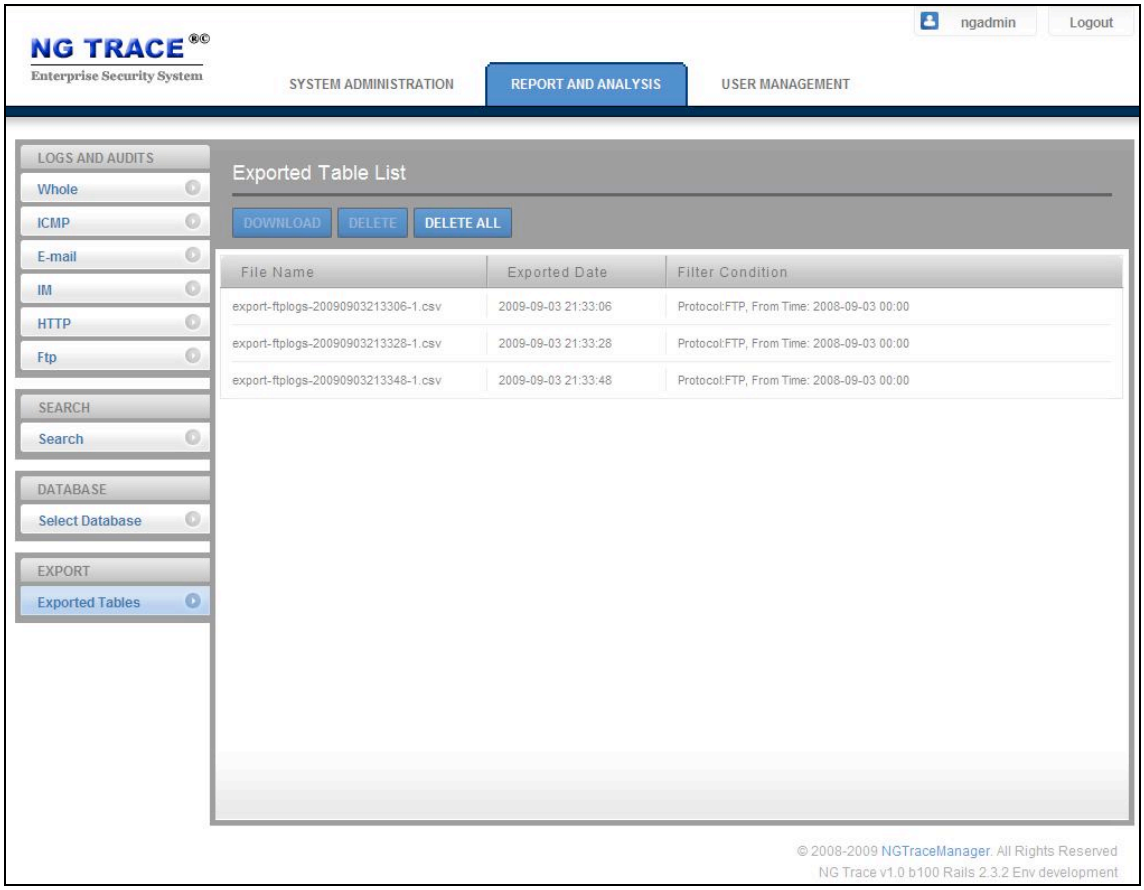

Figure 36. Export Table List

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.